Mathematisches Forschungsinstitut Oberwolfach

Report No. 51/2025

DOI: 10.4171/OWR/2025/51

Analytic Number Theory

Organized by
Kaisa Matomäki, Turku
James Maynard, Oxford
Kannan Soundararajan, Stanford
Trevor D. Wooley, West Lafayette

2 November – 7 November 2025

Abstract. Analytic number theory is a subject which continues to flourish and grow with several significant developments over the past few years making progress on some of the most famous open problems in mathematics. This workshop brought together world experts and young talent to discuss the various branches and recent developments in the subject.

Mathematics Subject Classification (2020): 11-06, 11Dxx, 11Lxx, 11Mxx, 11Nxx.

Introduction by the Organizers

The workshop Analytic Number Theory, organised by Kaisa Matomäki (Turku), James Maynard (Oxford), Kannan Soundararajan (Stanford), and Trevor Wooley (West Lafayette) was well attended with 47 participants from a broad geographic spectrum and wide mix of specialist research areas. In comparison to previous meetings, it was noticeable that there was a particularly high number of very strong younger researchers to complement established experts, which corresponds to the current energy and enthusiasm within the subject, and that many important breakthroughs have come from early career researchers. This balance in participants was reflected by a number of exciting talks on major results from participants who had only recently received their PhD.

Mehtaab Sawhney made an announcement of very significant progress (joint with Ben Green) on the 'anatomy of integers', describing the typical factorization of integers. Breakthrough work of Ford in the 2000s described the correct order

of magnitude for the number of integers with a divisor in a given dyadic interval, but by introducing several new ideas from random walks Green-Sawhney can now essentially refine this to an asymptotic formula – something which previously seemed totally out-of-reach.

Cedric Pilatte described his impressive recent work on the logarithmic 2-point Chowla conjecture using ideas from non-backtracking walks. As well as obtaining the strongest quantitative information that seems to be available with current techniques, this has already been the key input to further arithmetic consequences (as Joni Teräväinen described when talking about his joint with with Terence Tao).

Benjamin Bedert described his recent breakthrough on Chowla's famous cosine problem, showing that any combination of n cosines must take negative values as small as $-n^{-1/7}$, which is the first time polynomial bounds have been established for this 60 year old problem.

Katy Woo talked about her work on Manin's conjecture for Châtelet surfaces, explaining how delicate analytic estimates can overcome various different algebraic-geometric complications in this problem, ultimately obtaining an asymptotic formula for the growth of rational points on any Châtelet surface over $\mathbb{Q}$.

Alex Pascadi described his work on large sieve inequalities for Fourier coefficients of automorphic forms. By introducing new combinatorial ideas, he is able to prove stronger versions of these inequalities for the sorts of coefficients sequences that appear in many arithmetic applications. These are quantitatively strong enough that they can often be used as an unconditional substitute for Selberg's eigenvalue conjecture, allowing for stronger understanding of things like primes in arithmetic progressions.

All of the above speakers had only received their PhD within the past year (or were still a graduate student at the time of the workshop), and were participating for the first time. The exciting contributions made by new entrants was complemented by strong contributions from established researchers.

Valentin Blomer described new work (joint with Maksym Radziwiłł and Farrell Brumley) on an analytic approach to questions connected to the deep mixing conjecture of Michel and Venkatesh. Previous approaches to this conjecture have been based on ideas of ergodic theory, whereas the new analytic approach sidesteps some of the requirements needed for the ergodic methods to work. This relied on a very delicate understanding of various analytic aspects of the theory of automorphic forms.

Kevin Ford and Cécile Dartyge both described advances on questions connecting primes and sieves. Ford described his ongoing program with Maynard to attempt to understand the optimality and limitations of sieves for understanding the primes, while Dartyge described her work connecting sieves primes and digital questions.

Dan Petersen talked about his work on homological stability which allows one to obtain moments of L-functions over function fields. Although the connection between L-functions over function fields and geometric questions has been known for some time, this is essentially the first time that very sophisticated new ideas

in homotopy theory have been able to apply directly to questions coming from analytic number theory (beyond earlier work of Ellenberg-Venkatesh-Westerland). This exciting connection between the fields is surely set to grow.

Ben Green described a work (joint with Mehtaab Sawhney) on prime values of the form $p^2 + 4q^2$ with p, q prime, a result which had been searched for for a long time. This impressive work combined ideas from additive combinatorics (the theory of Gowers norms and concatenation theorems) with the traditional Type I/II sum technology from analytic number theory.

Beyond the talks, the workshop benefited from the 'Oberwolfach atmosphere'. Particularly since there were a number of strong junior researchers participating for the first time, the lively and collaborative atmosphere worked well at bringing people from across the subject together. Thomas Bloom led a problem session, and there were short talks which enabled participants who were not giving a main talk to introduce themselves and their research. Overall it was felt that there was a very good level of interaction, which made the workshop particularly successful.

Acknowledgement: The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-2230648, "US Junior Oberwolfach Fellows".

Workshop: Analytic Number Theory

Table of Contents

Abstracts

Representation of natural numbers as the sum of a square and a cube

Jörg Brüdern
(joint work with Robert C. Vaughan)

Let $U(N)$ denote the number of solutions of the diophantine equation

$$y_1^2 - y_2^2 = x_1^3 + x_2^3$$

with

$$1 \le y_j \le N^{1/2}, \quad 1 \le x_j \le N^{1/3}. \quad y_1 \ne y_2.$$

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

$$U(N) = CN^{2/3} \log N^{2/3} + O(N^{2/3} (\log\log N)^3).$$

This has applications to the number $r(n)$ of solutions to $x^3 + y^2 = n$ in positive integers. As an example, we are able to show that

$$\#\{n \le N : r(n) \ge 2\} \gg N^{1/3} / \log N.$$

This seems to be the first result showing that $r(n) \ge 2$ is a reasonably frequent event.

The constant C is a product of regularised local densities. In this sense, Theorem 1 resembles asymptotic formulae of Manin–Peyre type [1, 2, 3]. It has been suggested that the leading term in Theorem 1 should be given by the major arc contribution in a circle method approach to the underlying diophantine equation. If one carries this out, one is confronted with a number of surprises. To be more specific, let $Q \ge 1$, $R \ge 1$ and $QR \le N/2$. Then let M denote the union of the disjoint intervals of reals α satisfying $|q\alpha - a| \le Q/N$ with $1 \le a \le q \le R$ and $(a, q) = 1$. Further, write

$$f_j(\alpha) = \sum_{x \le N^{1/j}} e(\alpha x^j).$$

Theorem 2. *Fix a positive number A, and take $Q = AN^{1/3}$, $1 \le R \le N^{1/3}$. Then*

$$\int_M |f_2(\alpha) f_3(\alpha)|^2 = CN^{2/3} \log R + O(N^{2/3} (\log\log N)^3).$$

This misses the leading term in Theorem 1 by a factor $1/2$ if one chooses $R = N^{1/3}$. However, making the major arcs wider (larger Q) or higher (larger R), then the diagonal solutions $y_1 = y_2$ gradually invade the leading term.

Theorem 3. *Fix a positive number A, and take $Q = AN^{1/3}$, $R/N^{1/3} \to \infty$ and $R = o(N^{1/2} \log N)$. Then, there is a constant $D = D(A)$ with the property that*

$$\int_M |f_2(\alpha) f_3(\alpha)|^2 \sim DN^{2/3} \log N,$$

and D is increasing as a function of A and is unbounded.

In particular, the contribution from the major arcs is larger than $U(N)$ if A is chosen sufficiently large. The proof clearly shows that the effect is caused by the diagonal solutions. There are further results of this type, also for $R > N^{1/2}$ where the effect is even more pronounced.

References

[1] V. V. Batyrev and Y. I. Manin, *Sur le nombre des points rationnels de hauteur borné des variétés algébriques*, Math. Ann. **286** (1990), no. 1–3, 27–43.

[2] J. Franke, Y. I. Manin and Y. Tschinkel, *Rational points of bounded height on Fano varieties*, Invent. Math. **95** (1989), no. 2, 421–435.

[3] E. Peyre, *Hauteurs et mesures de Tamagawa sur les variétés de Fano*, Duke Math. J. **79** (1995), no. 1, 101–218.

Primes with almost prime reverse

Cécile Dartyge

(joint work with Joël Rivat and Cathy Swaenepoel)

Let $b \in \mathbb{N}$, $b \geq 2$. Any integer $n \in [b^{\lambda-1}, b^{\lambda}[$ with $\lambda \in \mathbb{N}$ has a base b representation of the form $n = \sum_{j=0}^{\lambda-1} \varepsilon_j(n) b^j$ where the digits $\varepsilon_j(n) \in \{0, \dots, b-1\}$ for all $0 \leq j \leq \lambda - 1$ and $\varepsilon_{\lambda-1}(n) \geq 1$. The reverse or mirror of such integer $n \in [b^{\lambda-1}, b^{\lambda} - 1]$, is the integer defined by

$$\overleftarrow{n} = \sum_{j=0}^{\lambda-1} \varepsilon_j(n) b^{\lambda-1-j}.$$

For example when $b = 10$, $\overleftarrow{13} = 31$, $\overleftarrow{37} = 73$. This definition of reverse depends on the choice of the base b but we won't precise this dependence when the context will be clear. The integers considered in the previous examples are prime numbers. Are there infinitely many prime numbers p whose reverse $\overleftarrow{p}$ is also a prime number? This is an open problem which seems at least as difficult as the twin prime conjecture.

An integer equal to its reverse is called a palindrome: 1234321 is a palindrome in base 10. Here again we conjecture the existence of infinitely many prime palindromes.

Col [1] in 2009 obtained the first progress towards this second conjecture. He proved the existence of infinitely many palindromes with few prime factors.

Let $\Omega(n)$ denote the number of prime factors of the integer n with multiplicity. Col proved that for any integer $b \geq 2$, there exists $k_b \in \mathbb{N}$ such that

$$\#\{n \leq x : \overleftarrow{n} = n \text{ and } \Omega(n) \leq k_b\} \gg_b \frac{\sqrt{x}}{\log x}. \tag{1}$$

Col's Theorem provides for each $b \geq 2$ an explicit admissible value of k_b. For example, $k_2 = 60$, $k_{10} = 372$. This result has been recently improved by Tuxanidy and Panario [7] who proved that for all b, (1) is valid with $k_b = 6$.

In [3], Martin, Rivat, Shparlinski, Swaenepoel and the author obtained such type of result for the binary reverse of the integers :

$$\#\{n \leq x : \max(\Omega(n), \Omega(\overleftarrow{n})) \leq 8\} \gg \frac{x}{(\log x)^2}.$$

Their result is given only in the base $b = 2$ but the proof can be adapted in all bases. The main result of this presentation shows the existence of infinitely many prime numbers with an almost prime reverse.

Theorem 1 (D., Rivat and Swaenepoel '25 [3]). *Let $b \geq 2$. There exists $\Omega_b \in \mathbb{N}$ such that for any $x \geq 5$, we have*

$$\#\{p \leq x : \Omega(\overleftarrow{p}) \leq \Omega_b\} \gg \frac{x}{(\log x)^2}.$$

The following values are admissible

$$\Omega_2 = 228, \Omega_3 = 333, \ldots, \Omega_{10} = 1378,$$

and when $b \to +\infty$ we may take

$$\Omega_b = 538.2b^2 + O(b).$$

This Theorem may be seen as an analogue of Renyi's Theorem for the Goldbach problem [6] saying that all sufficiently large even integer is the sum of a prime number and an almost prime number.

The proof of Theorem 1 employs some sieves. This yields us to study the distribution in arithmetic progressions of the reverses of the primes.

For any integers a, d, λ with $\lambda \geq 1$, $d \geq 2$ and any $t \in \mathbb{R}^+$ we consider the following counting functions:

$$\pi_\lambda(t) = \#\{b^{\lambda-1} \leq p < t\} \text{ and } \overleftarrow{\pi}_\lambda(t, a, d) = \#\{b^{\lambda-1} \leq p < t : \overleftarrow{p} \equiv a \mod d\}.$$

When $(d, b(b^2-1)) = 1$ it is natural to expect that $\overleftarrow{\pi}_\lambda(b^\lambda, a, d) \sim \frac{\pi_\lambda(b^\lambda)}{d}$. In the next Theorem, we show that this approximation holds on average on d. This result is a sort of Bombieri-Vinogradov Theorem for the reverses of the primes.

Theorem 2 (D., Rivat and Swaenepoel '25 [3]). *There exists an explicit $\xi_0 = \xi_0(b)$ such that for any given $\xi \in]0, \xi_0[$, there is some $c = c(b, \xi) > 0$ such that for any $\lambda \geq \lambda_0(b, \xi)$ we have*

$$\sum_{\substack{d \leq b^{\lambda\xi} \\ (d, b(b^2-1))=1}} \sup_{t \in [b^{\lambda-1}, b^\lambda]} \sup_{1 \leq a \leq d} \left| \overleftarrow{\pi}_\lambda(t, a, d) - \frac{\pi_\lambda(t)}{d} \right| \ll b^{\lambda - c\sqrt{\lambda}}.$$

Theorem 2 with the Richert's sieve weights [4] gives Theorem 1. Let Λ denote the van Mangoldt function. To prove Theorem 2, it is sufficient to bound sums of type

$$\sum_{b^{\lambda-1} \leq n < t} \Lambda(n) e\left(\frac{h\overleftarrow{n}}{d}\right),$$

on average on the fractions h/d with $1 \leq h \leq d$, $(h, d) = 1$, $D < d \leq 2D$ and the standard notation $e(u) = \exp(2i\pi u)$. After an application of the Vaughan identity,

we get type I and type II sums and as usual the type II sums are the most difficult to handle.

Following the Mauduit–Rivat method [5], we apply the van der Corput inequality which enables us to benefit of the carry propagation phenomenon. For almost all $(m,n) \in [b^\mu, b^{\mu+1}[\times[b^\nu, b^{\nu+1}[$ we have

$$\varepsilon_j(mn+mr) = \varepsilon_j(mn) \quad \forall (j,r) \in \{\mu+\varrho+\varrho', \dots, \mu+\nu-1\} \times \{1\dots, b^\varrho - 1\},$$

where ϱ, ϱ' are strictly positive parameters, small comparatively to μ and ν. To exploit this observation, it is convenient to introduce the modulo b^λ-reverse function:

$$R_\lambda(n) = \sum_{j=0}^{\lambda-1} \varepsilon_j(n) b^{\lambda-1-j}.$$

Writing $\mu_2 = \mu+\varrho+\varrho'$ we deduce that for almost m,n as above, we have:

$$R_\lambda(mn+mr) - R_\lambda(mn) = b^{\lambda-\mu_2}(R_{\mu_2}(mn+mr) - R_{\mu_2}(mn)).$$

We then need to bound sums of type

$$\sum_{b^{\nu-1}\le n<b^{\nu+1}} \left| \sum_{b^{\mu-1}\le m<b^\mu} e\left(\alpha b^{\lambda-\mu_2}(R_{\mu_2}(mn+mr) - R_{\mu_2}(mn)\right)\right|,$$

on average on the $\alpha = h/d$ for some exponents μ, ν satisfying $\mu+\nu = \lambda$, and $\mu \le \nu$. Since the function R_{μ_2} is b^{μ_2}-periodic, we can again employ exponential sums. The discrete Fourier transform associated to our problem has a nice product formula:

$$F_\lambda(\alpha,\beta) = \frac{1}{b^\lambda} \sum_{0\le n<b^\lambda} e(\alpha \overleftarrow{n} - \beta n) = \prod_{j=0}^{\lambda-1} K_b(\alpha b^{\lambda-j-1} - \beta b^j), \tag{2}$$

where K_b is the normalised Dirichlet kernel of length b: $K_b(t) = b^{-1}\sum_{u=0}^{b-1} e(ut)$.

One of our ingredients is an elimination trick. For any $\alpha, \beta \in \mathbb{R}$ we have $|F_\lambda(\alpha,\beta)| \le \min(G_{\lambda-1}^{1/2}(\alpha(b^2-1)), G_\lambda^{1/2}(\beta(b^2-1))$ with

$$G_\lambda(\alpha) = \prod_{j=0}^{\lambda-1} \left| K_b\left(\left\| \frac{\alpha b^j}{b+1} \right\|\right)\right|.$$

An important part of our work consists to obtain a collection of moments for the functions F_λ and G_λ. For example we prove for all $\kappa > 0$ the completely explicit bound:

$$\int_0^1 G_\lambda(\alpha)^\kappa \mathrm{d}\alpha \le \left(\frac{1}{b} + \sqrt{\frac{12(b+1)}{\pi(b-1)\kappa}}\right)^\lambda.$$

Such formulas are very useful for large values of κ. After some further manipulations we have to control some exponential sums in several variables. Most of these sums are sufficiently small but a critical part of them, "the extended diagonal terms" needs some new ideas to be handled. We succeed by using intensively the

product structure (2) and meticulously exploiting some diophantine restrictions of these critical sums.

References

[1] S. Col, *Palindromes dans les progressions arithmétiques*, Acta Arith., **137**, (2009), no. 1, 1–41.

[2] C. Dartyge, B. Martin, J. Rivat, I. E. Shparlinski and C. Swaenepoel, *Reversible primes*, J. Lond. Math. Soc. **109** (2024), no. 3, Paper No. e12883, 38.

[3] C. Dartyge, J. Rivat and C. Swaenepoel, *Prime numbers with an almost prime reverse*, preprint `arXiv:2506.21642v2` (2025).

[4] H. Halberstam and H.-R. Richert, *Sieve Methods* Academic Press, New York / London (1974).

[5] C. Mauduit and J. Rivat, *Sur un problème de Gelfond : la somme des chiffres des nombres premiers*, Ann. of Math., **171** (2010), no. 2, 1591–1646.

[6] A. Rényi, *On the representation of an even number as the sum of a single prime and single almost-prime number*, Izv. Akad. Nauk SSSR Ser. Mat., **12** (1948), 57–78.

[7] A. Tuxanidy and D. Panario, *Infinitude of palindromic almost-prime numbers*, Int. Math. Res. Not. IMRN (2024), no. 18, 12466–12503.

Distribution of mixed character sums and applications

Oleksiy Klurman

(joint work with J. Bober, B. Shala)

We will report on the results in [1] and [2]. We develop an approach aiming to understand the mixed character sums

$$S(\chi, x, \theta) = \sum_{n \le x} \chi(n) e(n\theta),$$

where χ is a (multiplicative) Dirichlet character mod q and $e(x) := e^{2\pi i x}$ is the additive character on $\mathbb{R}$. We are motivated by the following natural questions.

Problem 1. *For various ranges of parameters $q, x \to \infty$ determine the distribution of $S(\chi, x, \theta)$ as χ runs over a family of Dirichlet characters.*

Problem 2. *Let χ_q be a quadratic character. What is the limiting distribution of $S(\chi_q, x, \theta)$ when $\theta \in [0, 1]$ is chosen uniformly at random and $q \to \infty$?*

We consider for a prime q and a primitive (non-principal) Dirichlet character χ mod q the shifted-mixed character sum

$$\sum_{\alpha q < n < (\alpha+\beta)q} \chi(n) e(n\theta).$$

For each integer $k \in [0, q-1]$ and Dirichlet character χ, we define the function

$$F_{k,\chi,\alpha,\beta}(t) = \frac{e(-\alpha k)}{q^{1/2}} \sum_{\alpha q < n < (\alpha+\beta)q} \chi(n) e(n(k+t)/q),$$

a normalised version of the sum $S(\chi, \alpha, \beta, \theta)$, with $\theta = (k+t)/q$ and $t \in [0, 1)$. We regard $F_{k,q,\alpha,\beta} : \hat{\mathbb{F}}_q \to C[0, 1]$ as the discrete random process obtained by choosing

χ uniformly at random from the set of *all* characters mod q. We will consider the limiting behavior of $F_{k,q,\alpha,\beta}$ as $q \to \infty$ over the primes, with k either fixed or tending to infinity as well.

For each integer k we define the random process

$$F_{k,\alpha,\beta}(t) = \mathbf{X}\frac{e(\alpha t)}{2\pi i}\sum_{l\in\mathbb{Z}}\frac{e(\alpha l)e(\beta(l+t))-1)}{l+t}\mathbf{W}(k-l),$$

where $\mathbf{W}(l)$ is a completely multiplicative Steinhaus random variable and $\mathbf{X}$ is a random variable uniformly distributed on the unit circle, independent of $\mathbf{W}$. We introduce

$$F_{\alpha,\beta}(t) = \frac{e(\alpha t)}{2\pi i}\sum_{l\in\mathbb{Z}}\frac{e(\beta(l+t))-1}{l+t}\mathbf{X}(l),$$

where the $\mathbf{X}(l)$ are independent realizations of $\mathbf{X}$. Our first main result is the following convergence statement in the space of continuous functions $C[0,1]$.

Theorem 1. *Fix real numbers α and β. Then*

(1) *For each integer k, the sequence of random processes $F_{k,q,\alpha,\beta}$ converges in distribution to $F_{k,\alpha,\beta}$ as $q \to \infty$ over the primes.*
(2) *For each sequence $k_q \to \infty$ with $k_q = q^{o(1)}$, the sequence of random processes $F_{k_q,q,\alpha,\beta}$ converges in distribution to $F_{\alpha,\beta}$ as $q \to \infty$ over the primes.*
(3) *For each sequence $k_q \to \infty$ with $k_q = o(\pi(q))$, there is a full density subset $\mathcal{P}$ of the primes such that the sequence of random processes $F_{k_q,q,\alpha,\beta}$ converges in distribution to $F_{\alpha,\beta}$ as $q \in \mathcal{P}$ tends to infinity.*
(4) *For each irrational θ, there is a full density subset $\mathcal{P}_\theta$ of the primes such that the sequence of random processes $F_{\lfloor\theta q\rfloor,q,\alpha,\beta}$ converges in distribution to $F_{\alpha,\beta}$ as $q \in \mathcal{P}_\theta$ tends to infinity.*

We obtain the following immediate corollary.

Corollary 1. *For each irrational θ and real number β there is a full density subset $\mathcal{P}_\theta$ of the primes such that for every $t_0 \in [0,1]$, when $\{q\theta\} \to t_0$ for a sequence of $q \in \mathcal{P}_\theta$, the sequence*

$$\frac{1}{q^{1/2}}\sum_{n<\beta q}\chi(n)e(n\theta) \xrightarrow{d} F_{0,\beta}(t_0)$$

as χ varies over the characters mod q.

We now turn to Problem 2 and fix χ_q as the quadratic character mod q. We partition the interval $[0,1]$ into pieces $[\frac{k}{q}, \frac{k+1}{q})$ for $k \in [0, q-1]$ and our aim is to show that the behavior of the character sum $S(\chi,\alpha,\beta,\theta)$ in a randomly chosen subinterval is governed by an explicit random point process. For each prime q, let $G_{q,\alpha,\beta} : \{0,1,\dots,q-1\} \to C[0,1]$ be the random process $k \to \frac{q^{1/2}}{\tau(\chi_q)}F_{k,\chi_q,\alpha,\beta}(t)$, where the set $\{0,1,\dots,q-1\}$ is equipped with the uniform measure. Finally, we

introduce the random process

$$G_{\alpha,\beta}(t) = \frac{e(\alpha t)}{2\pi i} \sum_{l\in\mathbb{Z}} \frac{e(\alpha l)(e(\beta(l+t))-1)}{l+t} \mathbf{Y}(l),$$

where $\mathbf{Y}(l)$ are independent random variables uniformly distributed in $\{-1,1\}$.

Theorem 2. *For each fixed α and β, the random process $G_{q,\alpha,\beta}$ converges in distribution to $G_{\alpha,\beta}$ as $q\to\infty$ along the primes.*

We apply these results to deduce several applications. Our first application concerns a classical quantity of an algebraic polynomial $P\in\mathbb{C}[x]$. Recall the Mahler measure of P, defined as

$$M_0(P) := \exp\left(\int_0^1 \log|P(e(t))|dt\right).$$

In 1963, Mahler (also mentioned as Problem 10 by Borwein in his book) posed the following problem.

Problem 3 (Mahler Problem)**.** *What is*

$$b_m = \limsup_{n\to\infty} \frac{M_0(P_n)}{\sqrt{n}},$$

where $P_n(x) = \sum_{k=0}^n a_k x^k$ with $a_k = \pm 1$ for all k?

We apply our distributional results for incomplete exponential sums (Theorem 2) in conjunction with a new general method of dealing with the log-integrability problem to show the following result, improving the record in the Mahler problem.

Corollary 2. *There exist Littlewood polynomials of arbitrarily large degree with normalized Mahler measure $>.954$. Consequently, $b_m > .954$.*

References

[1] J.W. Bober, O. Klurman, B. Shala, *Distribution of mixed character sums and extremal problems for Littlewood polynomials*, preprint `arXiv:2510.06161` (2025).

[2] O. Klurman, Y. Lamzouri and M. Munsch, *L_q norms and Mahler measure of Fekete polynomials*, preprint `arXiv:2306.07156` (2023).

Log-saving bounds for two point logarithmic Chowla using non-backtracking matrices

Cédric Pilatte

Let λ be the Liouville function, defined as $\lambda(n) = (-1)^{\Omega(n)}$ where $\Omega(n)$ is the number of prime factors of n counted with multiplicity. Chowla's conjecture predicts that, for any fixed distinct integers $h_1,\dots,h_k$,

$$\sum_{n\le X} \lambda(n+h_1)\cdots\lambda(n+h_k) = o(X) \quad \text{as } X\to\infty.$$

This is a multiplicative analogue of the Hardy–Littlewood conjecture on correlations of the von Mangoldt function. Although generally regarded as less difficult, Chowla's conjecture also faces the well-known *parity obstruction* in analytic number theory, and is wide open for any $k \geq 2$.

Nevertheless, remarkable progress has been made on weaker variants of Chowla's conjecture in the last decade. Specifically, the *logarithmic* version of Chowla's conjecture, which asserts that

$$\sum_{n \leq X} \frac{1}{n} \lambda(n+h_1) \cdots \lambda(n+h_k) = o(\log X) \quad \text{as } X \to \infty \tag{1}$$

for any distinct $h_1, \ldots, h_k$, has seen significant advances. It was established for $k = 2$ by Tao [3], and for all odd k by Tao and Teräväinen [4], using an *entropy decrement argument*. Proving (1) for even integers $k \geq 4$ remains an important open problem, intimately linked to Sarnak's conjecture on zero-entropy dynamical systems.

In this talk, we focus on quantitative bounds for (1) in the case of two-point correlations. Tao's method [3] yields an explicit bound of the form

$$\sum_{n \leq X} \frac{1}{n} \lambda(n)\lambda(n+1) \ll \frac{\log X}{(\log\log\log\log X)^c}$$

for some absolute constant $c > 0$. The entropy method can be refined to obtain a triply iterated logarithm in the denominator (see [4]). In 2021, Helfgott and Radziwiłł [1] introduced a novel approach based on spectral expander techniques, and proved the stronger estimate

$$\sum_{n \leq X} \frac{1}{n} \lambda(n)\lambda(n+1) \ll \frac{\log X}{(\log\log X)^{1/2}}. \tag{2}$$

In [5], we improve this further to

$$\sum_{n \leq X} \frac{1}{n} \lambda(n)\lambda(n+1) \ll (\log X)^{1-c}, \tag{3}$$

where $c > 0$ is an absolute constant. It appears that saving a fixed power of the logarithm is the best achievable result with current techniques. Our proof builds on the strategy of Helfgott and Radziwiłł, but requires new ingredients, including non-backtracking operators and a refined combinatorial analysis.

We briefly outline the approach of Helfgott and Radziwiłł [1]. Let N be a large parameter, and let $\mathcal{P}$ be the set of primes in the interval $[H_0, H]$, where $H_0 = \exp((\log N)^{1/3})$ and $H = \exp((\log N)^{1/2-\varepsilon})$. The key estimate proved by Helfgott and Radziwiłł is

$$\sum_{n \in (N,2N]} \sum_{p \in \pm\mathcal{P}} \left(\mathbf{1}_{p|n} - \frac{1}{p} \right) \lambda(n)\lambda(n+p) \ll N \Big(\sum_{p \in \mathcal{P}} \frac{1}{p} \Big)^{1/2}, \tag{4}$$

thus saving a factor $(\sum_{p\in\mathcal{P}}\frac{1}{p})^{1/2} \asymp (\log\log N)^{1/2}$ over the trivial bound. The result (4), together with an exponential sum estimate of Matomäki, Radziwiłł, and Tao [2], implies doubly logarithmic savings for the logarithmic Chowla sum (2).

To prove (4), Helfgott and Radziwiłł analyse the matrix $B = (b_{m,n})_{m,n\in(N,2N]}$ defined by

$$b_{m,n} := \begin{cases} \mathbf{1}_{p|n} - \frac{1}{p} & \text{if } |m-n| = p \text{ for some } p \in \mathcal{P}, \\ 0 & \text{otherwise.} \end{cases}$$

They show that, after altering a small number of rows and columns of B, the resulting matrix $\widetilde{B}$ satisfies the trace bound

$$\operatorname{Tr}(\widetilde{B}^{2k}) \le e^{O(k)} N \Big(\sum_{p\in\mathcal{P}} \frac{1}{p} \Big)^k \tag{5}$$

where the integer k can be taken as large as $\log H$. The proof of (5) is combinatorial, expanding the trace as a sum over all closed walks of length $2k$ on a weighted graph with adjacency matrix B. A linear algebra argument then shows that the trace bound (5) implies (4); in fact, this deduction only uses that λ is 1-bounded.

To obtain logarithmic savings for two-point Chowla, we replace the set $\mathcal{P}$ of primes by a much denser set $\mathcal{D}$ of integers, where each $d \in \mathcal{D}$ is a product of $\asymp \log\log N$ primes. We prove the following analogue of (4):

$$\sum_{n\in(N,2N]} \sum_{d\in\pm\mathcal{D}} \prod_{p|d} \Big(\mathbf{1}_{p|n} - \frac{1}{p} \Big) \lambda(n)\lambda(n+d) \ll N \Big(\sum_{d\in\mathcal{D}} \frac{1}{d} \Big)^{1/2+o(1)}. \tag{6}$$

The set $\mathcal{D}$ is chosen so that $\sum_{d\in\mathcal{D}} 1/d$ is a fixed power of $\log N$. Our problem thus reduces to studying the matrix $A = (a_{m,n})_{m,n\in(N,2N]}$ defined by

$$a_{m,n} := \begin{cases} \prod_{p|d} \left(\mathbf{1}_{p|n} - \frac{1}{p} \right) & \text{if } |m-n| = d \text{ for some } d \in \mathcal{D}, \\ 0 & \text{otherwise.} \end{cases}$$

Unfortunately, the techniques of Helfgott and Radziwiłł for proving the trace bound (5) do not directly generalise to this matrix A.

Our first key idea is to consider the *non-backtracking operator* M associated to A. This is a linear operator acting on directed edges of a weighted graph with adjacency matrix A, which encodes walks that cannot immediately retrace their steps. We proceed in two stages.

We first prove a trace bound analogous to (5) for a slight perturbation $\widetilde{M}$ of the non-backtracking operator M: for $k \asymp \log H$ we show that

$$\operatorname{Tr}\Big((\widetilde{M}^k)^* \widetilde{M}^k \Big) \le N \Big(\sum_{d\in\mathcal{D}} \frac{1}{d} \Big)^{(1+o(1))k}. \tag{7}$$

The proof of (7) is the most technical part of the paper; the fact that the integers in $\mathcal{D}$ have many prime factors creates major complications. The left-hand side of (7) can be expanded in terms of walks of length $2k$ that are mostly non-backtracking (a crucial property in the analysis).

- Walks with essentially independent steps (meaning that the integers in $\mathcal{D}$ used along the walk share very few prime factors) exhibit a lot of cancellation; their contribution to the trace is negligible.
- The remaining walks have many dependencies between their steps. We further classify these walks according to a measure of complexity, which we call *unpredictability*. Roughly speaking, a walk is unpredictable if, at many steps along the walk, there are many possible choices for the next step given the past history of the walk. We show that unpredictable walks also contribute little to the trace, using combinatorial arguments. The remaining *predictable* walks are very structured, and their contribution constitutes the main term in (7).

In the second stage, we relate the spectral properties of the modified non-backtracking operator $\widetilde{M}$ to those of the original matrix A. Our main tool here is the *Ihara–Bass formula*: in an unweighted graph with adjacency and non-backtracking matrices A_0 and M_0, this is the classical identity

$$\det(I - uM_0) = \det(I - uA_0 + u^2(D_0 - I)) \cdot P(u) \quad \text{for all } u \in \mathbb{C},$$

where D_0 is the diagonal degree matrix and $P(u)$ is an explicit polynomial factor. Using a weighted version of this formula, we control the eigenvalues of A in terms of those of $\widetilde{M}$. The quadratic term in the Ihara–Bass formula complicates matters, but a continuity argument based on Cauchy's interlacing theorem allows us ultimately to deduce the desired bound (6) which, in turn, implies the claimed bound (3) on logarithmic Chowla correlations.

References

[1] Harald A. Helfgott and Maksym Radziwiłł, *Expansion, divisibility and parity*, preprint `arXiv:2103.06853` (2021).

[2] Kaisa Matomäki, Maksym Radziwiłł, and Terence Tao, *An averaged form of Chowla's conjecture*, Algebra Number Theory **9** (2015), no. 9, 2167–2196.

[3] ———, *The logarithmically averaged Chowla and Elliott conjectures for two-point correlations*, Forum of Mathematics, Pi **4** (2016), e8.

[4] Terence Tao and Joni Teräväinen, *Odd order cases of the logarithmically averaged Chowla conjecture*, Journal de Théorie des Nombres de Bordeaux **30** (2018), no. 3, 997–1015.

[5] Cédric Pilatte, *Improved bounds for the two-point logarithmic Chowla conjecture*, preprint `arXiv:2310.19357` (2025).

Analytic approaches to joint equidistribution

Valentin Blomer

(joint work with Farrell Brumley and Maksym Radziwiłł)

A landmark equidistribution theorem [3, 5] states that integral points on spheres of growing radius

$$R_d := \frac{1}{\sqrt{d}}\{\mathbf{x} \in \mathbb{Z}^3 \mid (x_1, x_2, x_3) = 1, x_1^2 + x_2^2 + x_3^2 = d\} \subseteq \mathbb{S}^2$$

become equidistributed as long as the necessary congruence conditions $d \not\equiv 0, 4, 7 \pmod 8$ are satisfied. Each $x \in \sqrt{d}R_d$ can be interpreted as an integral traceless quaternion and (for squarefree d) defines an embedding of $E = \mathbb{Q}(\sqrt{-d})$ in the rational quaternions $\mathcal{H}(\mathbb{Q})$. In this way, we obtain a simply transitive action of the class group $\mathcal{C}_d$ of $\mathbb{Q}(\sqrt{-d})$ on a finite quotient of $\tilde{R}_d = R_d/\Gamma$ with $|\Gamma| \le 24$. In modern terminology, the equidistribution statement can be rephrased as the equidistribution of an adelic torus orbit of large discriminant inside the adelic quotient of an inner or outer form of PGL_2.

In their ICM address, Michel and Venkatesh [8] introduced a new generation of joint equidistribution problems where a quadratic field is embedded simultaneously into two quaternion algebras. We refer to [2] for an exact statement of the simultaneous equidistribution conjecture in general, as well as for many classical instances of it, and restrict ourselves here to two typical examples.

Example 1: Consider the integral points on the ellipsoid

$$R'_d := \frac{1}{\sqrt{d}}\big\{\mathbf{x} \in \mathbb{Z}^3 \mid (x_1, x_2, x_3) = 1, 2x_1^2 + 5x_2^2 + 10x_3^2 = d\big\} \subseteq \mathbb{E}.$$

Again $\mathcal{C}_d$ acts simply transitively on some finite quotient $\tilde{R}'_d = R'_d/\Gamma'$, and after fixing base points $x_0 \in R_d$, $x'_0 \in R'_d$, we can consider the pairs

$$\{([\mathfrak{a}] \cdot x_0, [\mathfrak{a}] \cdot x'_0) \mid [\mathfrak{a}] \in \mathcal{C}_d\} \subseteq \mathbb{S}^2/\Gamma \times \mathbb{E}/\Gamma'$$

and ask whether this equidistributes as $d \equiv 1, 2 \pmod 4$, $d \equiv 0, 2, 3 \pmod 5$ squarefree, $d \to \infty$.

Example 2: For $x \in \sqrt{d}R_d$ consider the rank 2 lattice $x^\perp \cap \mathbb{Z}^3$ of discriminant d. After suitable rotation and scaling, we can identify it with a Heegner point $\Lambda_x \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ and ask whether the pair $\{(x, \Lambda_x) \mid x \in \sqrt{d}R_d\} \subseteq \mathbb{S}^2 \times \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ equidistributes.

There are various ways to attack such problems. Ergodic theory provides powerful methods (see e.g. [1, 6]) which however depend on the choice of two (arbitrary) primes p_1, p_2 and the restriction to d such that p_1, p_2 split in $\mathcal{O}_E$ with $E = \mathbb{Q}(\sqrt{-d})$. Varying p_1, p_2 in finitely many ways, there will remain a positive proportion of d that are not covered by this argument. Here we give a brief overview of an analytic approach.

The starting point is a Weyl sum as in [2] with a test function f_i, $i = 1, 2$, on each of the two quaternion algebras under consideration. If both f_1, f_2 are cuspidal with Hecke eigenvalues $\lambda_1(n), \lambda_2(n)$, after an application of Waldspurger's theorem we are led to estimating expressions of the type

$$\frac{1}{\#\mathcal{C}_d} \sum_{\chi \in \hat{\mathcal{C}}_d} \frac{\sqrt{L(1/2, f_1 \times \chi) L(1/2, f_2 \times \chi)}}{L(1, \chi_d)} \tag{1}$$

where the square roots are understood as "canonical square roots", i.e. they are periods and can have either sign. A direct application of the Cauchy–Schwarz would not work, but one can first insert as a mollifier Dirichlet polynomials that resemble $\sqrt{L(1/2, f_1 \times \chi)/L(1/2, f_2 \times \chi)}$ resp. $\sqrt{L(1/2, f_2 \times \chi)/L(1/2, f_1 \times \chi)}$. This is

inspried by [10]. If f_2, say, is an Eisenstein series, one has to argue somewhat differently. For this presentation we restrict ourselves to analyzing the cuspidal moment (1). To this end, we need the following three results.

Theorem 1. *For an ideal $\mathfrak{n} \subseteq \mathcal{O}_E$ coprime to d and the level of f we have*

$$\frac{1}{\#\mathcal{C}_d} \sum_{\chi \in \hat{\mathcal{C}}_d} \frac{L(1/2, f \times \chi)\chi(\mathfrak{n})}{L(1, \chi_d)} = \lambda(\mathfrak{n}) + O(\mathrm{Nr}(\mathfrak{n})^A d^{-\delta})$$

for constants $A, \delta > 0$ and some explicit arithmetic function λ.

The proof is based on a spectral decomposition which leads to a certain spectral reciprocity formula. In this way one can bound (1) by an expression roughly of the shape

$$\exp\Big(-\frac{1}{4} \sum_{\substack{p \leq d^{1/1000} \\ \chi_d(p)=1}} \frac{(\lambda_1(p) - \lambda_2(p))^2}{p}\Big).$$

Theorem 2. *Let π_1, π_2 be cuspidal automorphic representations of $\mathrm{PGL}_2/\mathbb{Q}$ with Hecke eigenvalues λ_i. Assume that $\mathrm{sym}^k \pi_1$ and $\mathrm{sym}^k \pi_2$ are cuspidal and distinct for $k = 2, 3, 4$. Then*

$$\sum_{\substack{p \leq X \\ |\lambda_1(p) - \lambda_2(p)| \geq 10^{-10}}} \log p \geq 0.508X$$

for all sufficiently large $X \geq X_0$.

The proof optimizes the available information on functoriality (cf. [7]), and it is crucial for our application to obtain a constant bigger than $1/2$.

Finally we need to understand the distribution of small split primes in relation to zeros of quadratic Dirichlet L-functions; cf. also [9]. For a function $1 \leq \psi(D) \leq o(\log D)$ tending to infinity, we shall say that the negative fundamental discriminant $-D$ is *ψ-good* if $L(s, \chi_D)$ has no zero in the region

$$\Re s \geq 1 - \frac{20\psi(D)\log\psi(D)}{\log D}, \quad |\Im s| \leq \frac{2\psi(D)^2}{\log D}. \tag{2}$$

We think of ψ as growing arbitrarily slowly, so that (2) can be seen as an $o(1)$-strengthening of a no Siegel zero condition.

Theorem 3. *Let $1 \leq \psi(D) \leq o(\log D)$ be a function tending to infinity. Then for any fixed $\delta < 1/2$ and any sufficiently large ψ-good negative fundamental discriminant $-D$ we have*

$$\sum_{\substack{X \leq p \leq X^2 \\ \chi_D(p)=1}} \frac{1}{p} \geq \delta \sum_{X \leq p \leq X^2} \frac{1}{p},$$

uniformly for $X \geq D^{1/\psi(D)}$.

Our main result is

Theorem 4. *The simultaneous equidistribution conjecture holds at almost maximal level for all ψ-good discriminants D with a convergence rate of $O(\psi(D)^{-\rho})$ for some $\rho > 0$.*

A density estimate [4] shows that not only does Theorem 4 apply to 100% of all discriminants, but the cardinality of the exceptional set of discriminants in a given dyadic interval may grow arbitrarily slowly.

References

[1] M. Aka, M. Einsiedler, U. Shapira, *Integer points on spheres and their orthogonal lattices*, Invent. Math. **206** (2016), 379–396.

[2] V. Blomer, F. Brumley, *Simultaneous equidistribution of toric periods and fractional moments of L-functions*, J. Eur. Math. Soc. **26** (2024), 2745–2796.

[3] W. Duke, R. Schulze-Pillot, *Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids*, Invent. Math. **99** (1990), 49–57.

[4] P. Gallagher, *A large sieve density estimate near $\sigma = 1$*, Invent. Math. **11** (1970), 329–339.

[5] E.P. Golubeva, O.M. Fomenko, *Asymptotic distribution of lattice points on the three- dimensional sphere.* Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. **160** (1987), 54–71, 297 (in Russian); English transl.: J. Soviet Math. **52** (1990), 3036–3048.

[6] I. Khayutin, *Joint equidistribution of CM points*, Annals of Math. **189** (2019), 145–276.

[7] H. Kim, F. Shahidi, *Cuspidality of symmetric powers with applications*, Duke Math. J. **112** (2002), 177–197.

[8] P. Michel, A. Venkatesh, *Equidistribution, L-functions and ergodic theory: on some problems of Yu. Linnik*, Intern. Congr. Math. II, 421-457, Eur. Math. Soc. 2006.

[9] H. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Mathematics **84** (1994), 220 pp.

[10] M. Radzwiłł, K. Soundararajan, *Moments and distribution of central values of quadratic twists of elliptic curves*, Invent. Math. **202** (2015), 1029–1068.

The "multilinear circle method" and pointwise ergodic theory

Sarah Peluse

(joint work with Dariusz Kosz, Mariusz Mirek, and James Wright)

Let $(X, \mathcal{B}, \mu)$ be a probability space and $T : X \to X$ be an invertible measure-preserving transformation. In the early 1930s, von Neumann [11] and Birkhoff [3] proved, respectively, that for all $f \in L^\infty(X)$ (a condition that can be weakened) the classical ergodic average

$$\frac{1}{N}\sum_{n=1}^{N} f(T^n x)$$

converges both in $L^2(X)$ and pointwise for almost every $x \in X$. It is now a fundamental problem in ergodic theory to determine whether analogues of these results hold for "nonconventional ergodic averages", the first examples of which arose in 1977 in Furstenberg's [8] alternative proof of Szemerédi's 1975 theorem [14] on arithmetic progressions in dense sets of integers. Shortly after the proof of a

multidimensional polynomial generalization of Szemerédi's theorem by Bergelson and Leibman [2] in 1996, Bergelson [1] posed the following concrete question:

Question 1. *Let $m \in \mathbb{N}$ and $(X, \mathcal{B}, \mu)$ be a probability space endowed with a family of commuting invertible measure-preserving transformations $T_1, \dots, T_m : X \to X$. Let $P_1, \dots, P_m \in \mathbb{Z}[y]$. Is it true that for any functions $f_1, \dots, f_m \in L^\infty(X)$ the multilinear polynomial ergodic averages*

$$\frac{1}{N} \sum_{n=1}^{N} \prod_{i=1}^{m} f_i \left(T_i^{P_i(n)} x \right), \qquad x \in X, \tag{1}$$

converge both in $L^2(X)$ and pointwise almost everywhere on X as $N \to \infty$?

The convergence of the averages (1) in $L^2(X)$ is now known in full generality (in fact, in even greater generality than the setting of Question 1) thanks to work of Walsh [15] in 2012, but pointwise convergence is still almost completely open. Until recently, pointwise almost everywhere convergence was only known for the nonconventional ergodic averages

$$\frac{1}{N} \sum_{n=1}^{N} f(T^{P(n)} x) \tag{2}$$

when $\deg P > 1$ and

$$\frac{1}{N} \sum_{n=1}^{N} f_1(T^{an} x) f_2(T^{bn} x)$$

when a and b are any nonzero integers, both of which were handled in work of Bourgain [4, 5, 6, 7] in 1988 and 1990.

Bourgain's proof of the pointwise almost everywhere convergence of (2) crucially uses the circle method, and one of the major obstructions to generalizing his argument to multilinear (i.e., with $m \geq 2$) polynomial ergodic averages was the lack of a suitable replacement for the use of Weyl's inequality. A strong enough replacement in certain cases was proven recently by the speaker and Prendiville [13, 12] in their work on quantitative analogues of the Bergelson–Leibman theorem, and classifies bounded functions $f_0, f_1, f_2 : \mathbb{Z} \to \mathbb{C}$ with support in $\{1, \dots, N^2\}$ for which

$$\left| \sum_{x \in \mathbb{Z}} \sum_{y=1}^{N} f_0(x) f_1(x+y) f_2(x+P(y)) \right| \geq \delta N^3$$

when $\deg P > 1$. In 2022, Krause, Mirek, and Tao [10] used these results to prove pointwise almost everywhere convergence of the bilinear polynomial averages

$$\frac{1}{N} \sum_{n=1}^{N} f_1(T^n x) f_2(T^{P(n)} x)$$

when $\deg P > 1$.

This talk concerned very recent work of the speaker with Kosz, Mirek, and Wright [9] proving pointwise almost everywhere convergence of (1) in a large number of new cases:

Theorem 1 (Kosz, Mirek, P., and Wright '25+ [9])**.** *Let $(X, \mathcal{B}, \mu)$ be a probability space endowed with commuting measure-preserving transformations $T_1, \dots, T_m : X \to X$ and $P_1, \dots, P_m \in \mathbb{Z}[y]$ have distinct degrees. For any $f_1, \dots, f_m \in L^\infty(X)$, the multilinear polynomial ergodic average* (1) *converges pointwise almost everywhere on X as $N \to \infty$.*

References

[1] V. Bergelson, *Ergodic Ramsey Theory – an update, Ergodic Theory of $\mathbb{Z}^d$-actions* (edited by M. Pollicott and K. Schmidt), London Math. Soc. Lecture Note Series **228** (1996), pp. 1–61.

[2] V. Bergelson, A. Leibman, *Polynomial extensions of van der Waerden's and Szemerédi's theorems*, J. Amer. Math. Soc. **9** (1996), pp. 725–753.

[3] G. Birkhoff, *Proof of the ergodic theorem*, Proc. Natl. Acad. Sci. USA **17** (1931), no. 12, pp. 656–660.

[4] J. Bourgain, *On the maximal ergodic theorem for certain subsets of the integers*, Israel J. Math. **61** (1988), pp. 39–72.

[5] J. Bourgain, *On the pointwise ergodic theorem on L^p for arithmetic sets*, Israel J. Math. **61** (1988), pp. 73–84.

[6] J. Bourgain, *Pointwise ergodic theorems for arithmetic sets*, with an appendix by J. Bourgain, H. Furstenberg, Y. Katznelson, and D.S. Ornstein, Inst. Hautes Etudes Sci. Publ. Math. **69** (1989), pp. 5–45.

[7] J. Bourgain, *Double recurrence and almost sure convergence*, J. Reine Angew. Math. **404** (1990), pp. 140–161.

[8] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Anal. Math. **31** (1977), pp. 204–256.

[9] D. Kosz, M. Mirek, S. Peluse, J. Wright, *The multilinear circle method and a question of Bergelson*, preprint `arXiv:2411.09478` (2025).

[10] B. Krause, M. Mirek, T. Tao, *Pointwise ergodic theorems for non-conventional bilinear polynomial averages*, Ann. of Math. **195** (2022), no. 3, pp. 997–1109.

[11] J. von Neumann, *Proof of the quasi-ergodic hypothesis*, Proc. Natl. Acad. Sci. USA **18** (1932), pp. 70–82.

[12] S. Peluse, *Bounds for sets with no polynomial progressions*, Forum Math. Pi. (2020), article no. e16.

[13] S. Peluse, S. Prendiville, *Quantitative bounds in the non-linear Roth theorem*, Invent. Math. **238** (2024), no. 3, 865–903.

[14] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), pp. 199–245.

[15] M. Walsh, *Norm convergence of nilpotent ergodic averages*, Ann. of Math. **175** (2012), no. 3, pp. 1667–1688.

Moments in families of L-functions over function fields via homological stability

Dan Petersen
(joint work with Bergström–Diaconu–Westerland and Miller–Patzt–Randal-Williams)

The following conjecture is due to Conrey–Farmer–Keating–Rubinstein–Snaith [1]:

Conjecture 1. *Let $\zeta(s)$ be Riemann's zeta-function. For each integer $k \geq 1$ there exists an explicit polynomial P_k of degree k^2 such that*

$$\frac{1}{T}\int_0^T |\zeta(\tfrac{1}{2}+it)|^{2k}\mathrm{d}t = P_k(\log T) + o(1).$$

In fact, this conjecture is a special case of a general "recipe" that is supposed to apply also to moments in *families of L-functions*. One well-studied family is the quadratic family:

Conjecture 2. *For each integer $k \geq 1$ there exists an explicit polynomial Q_k of degree $k(k+1)/2$ such that*

$$\frac{1}{N}\sum_{\substack{|d|\leq N\\ d \text{ squarefree}}} L(\tfrac{1}{2},\chi_d)^k = Q_k(\log N) + o(1).$$

Conjecture 2 admits an exact function-field analogue.

Conjecture 3. *Let q be an odd prime power. For each integer $k \geq 1$ there exists an explicit polynomial $R_{k,q}$ of degree $k(k+1)/2$ such that*

$$\frac{1}{q^{2g+1}}\sum_{\substack{d\in\mathbf{F}_q[t]\\ d \text{ squarefree, monic}\\ \deg d = 2g+1}} L(\tfrac{1}{2},\chi_d)^k = R_{k,q}(g) + o(1).$$

The goal of the two papers [2, 3] is to prove Conjecture 3 for q sufficiently large with respect to k, using methods of homological stability and homotopy theory. More explicitly, we prove the equality in Conjecture 3 with an error term of the form $O(4^{g(k+1)}q^{-Ag+B})$, with A and B positive constants. Once q is large enough, we get a power-saving error term. In particular, the error term is good enough that we "see" all coefficients of all the polynomials R_k. This is perhaps the strongest vindication yet that the Conrey–Farmer–Keating–Rubinstein–Snaith "recipe" is correct.

Here are some ideas of the proof. The left-hand side of Conjecture 3 can be interpreted homologically, by the Grothendieck–Lefschetz trace formula, as

$$\mathrm{Tr}\big(\mathrm{Frob}_q \mid H_*^{\acute{e}t}(\mathrm{Conf}_{2g+1}(\mathbb{A}^1)_{\overline{\mathbf{F}}_q}; \mathcal{L}_k)\big),$$

where $\mathrm{Conf}_n(\mathbb{A}^1)$ is the configuration space of n distinct unordered points on the affine line,[1] and $\mathcal{L}_k$ is a certain smooth ℓ-adic sheaf, depending on k. The sheaf $\mathcal{L}_k$ lifts to characteristic zero, and one has a comparison isomorphism

$$H_*^{\acute{e}t}(\mathrm{Conf}_{2g+1}(\mathbb{A}^1)_{\overline{\mathbf{F}}_q}; \mathcal{L}_k) \cong H_*^{sing}(\mathrm{Conf}_{2g+1}(\mathbf{C}); \mathcal{L}_k).$$

Furthermore, the cohomology of $\mathrm{Conf}_n(\mathbf{C})$ is just the group cohomology of the Artin braid group β_n. At this point, we are now considering a problem in algebraic topology: the left-hand side of Conjecture 3 is expressed as a question about homology of braid groups as the number of strands goes to infinity.

This is exactly the type of question that *homological stability* aims to answer: what is the homology in a sequence of groups G_n, asymptotically, as the parameter n goes to infinity? Typically, computing the homology of an individual group G_n is very difficult, but computing the *stable homology* — the limiting value as n goes to infinity — is much more tractable. This is also what happens here. Moreover:

- The trace of Frobenius on stable homology, suitably interpreted, gives rise to the main term $R_k(g)$ in Conjecture 3. We can compute this.
- The trace of Frobenius on unstable homology gives rise to the error term. We can control this if we know a bound on unstable Betti numbers (this turns out to be easy) and a good enough range of stability.

The sheaf $\mathcal{L}_k$ decomposes into summands V_λ, indexed by irreducible representations of the symplectic group. The multiplicity of V_λ in $\mathcal{L}_k$ depends on k and n, but the family of summands $\{V_\lambda\}$ are the same regardless.[2] It is thus natural to study each summand $H_*(\beta_n; V_\lambda)$ individually.

What is done in [2]**.** A very general stability theorem of Randal-Williams–Wahl [4] implies that the sequence $H_*(\beta_n; V_\lambda)$ satisfies homological stability:

(1) $\quad H_k(\beta_n; V_\lambda) \to H_k(\beta_{n+1}; V_\lambda)$ is an isomorphism for $k < \frac{1}{2}(n - |\lambda|)$.

It is thus meaningful to ask what the stable homology of $H_*(\beta_n; V_\lambda)$ is. We compute the stable homology, together with its action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. We show that the answer is compatible with Conjecture 3, but that the range of stability (1) is not good enough to imply Conjecture 3. We show that Conjecture 3 would follow from our topological calculations if we knew a stable range of the form

(2) $\quad H_k(\beta_n; V_\lambda) \to H_k(\beta_{n+1}; V_\lambda)$ is an isomorphism for $k < An - B$;

what we call a "uniform stability bound".

[1] Equivalently, the moduli space of squarefree monic polynomials of degree n.

[2] The polynomial dependence on n in Conjecture 3 arises only from this: the multiplicity of V_λ in $\mathcal{L}_k$ is given by a degree $k(k+1)/2$ polynomial in n.

What is done in [3]**.** We prove (2). Almost all prior work on homological stability with twisted coefficients has focused on stability for *polynomial coefficient systems*. Easy examples show that for a typical polynomial coefficient system, the stable range depends on the degree of polynomiality. The V_λ are polynomial of degree $|\lambda|$, which gives rise to the dependence on $|\lambda|$ in (1). We thus need a new approach, not relying on polynomiality. The idea is that the coefficients V_λ are "pulled back" from the family of groups $\{\mathrm{Sp}_{2g}(\mathbf{Z})\}$, and on this family of groups they all have a uniform stable range by Borel's work on stable real cohomology of arithmetic groups [5]. We prove a general theorem that allows you to "propagate" a stable range when pulling back a coefficient system from one family of groups to another, under certain conditions which are in particular satisfied here.

Remark. An advantage of working in the function field setting is that there is an additional parameter q that you can vary, and you can simplify your problem by increasing q. This has been used previously by Katz–Sarnak to show the $q \to \infty$ limit of Conjecture 3. Then, Frobenius eigenvalues equidistribute according to a theorem of Deligne, and this allows you to prove e.g. that sums which should have lots of cancellation do have lots of cancellation. What we do in [2, 3] is also to exploit the freedom of varying q, but in a different way. Namely, Deligne's bounds on Frobenius eigenvalues show that if X is smooth then eigenvalues on $H_i(X)$ always have absolute value between $q^{-i/2}$ and q^{-i}. So by taking q large, the effect of H_i for large i can be made arbitrarily small, and low-degree homology will dominate. On the other hand, homological stability allows you to compute $H_i(X)$ for small i. This means that we never have to prove any cancellation — the dominant term comes from low-degree homology, which we completely understand. This is what allows us to fix a particular value of q in Conjecture 3, as opposed to taking the limit first as $q \to \infty$.

Remark. We do not only prove a formula for moments, but for shifted moments. The same methods also allow for asymptotics for ratios, if one bounds the distance from the critical line: this is an insight of Wang [6].

References

[1] J. B. Conrey, D. W. Farmer, J. P. Keating, M. O. Rubinstein and N. C. Snaith, *Integral moments of L-functions*, Proc. London Math. Soc. (3) **91** (2005), no. 1, 33–104.

[2] J. Bergström, A. Diaconu, D. Petersen and C. Westerland, *Hyperelliptic curves, the scanning map, and moments of families of quadratic L-functions*, preprint `arXiv:2302.07664` (2023).

[3] J. Miller, P. Patzt, D. Petersen and O. Randal-Williams, *Uniform twisted homological stability*, preprint `arXiv2402.00354` (2024).

[4] O. Randal-Williams and N. Wahl, *Homological stability for automorphism groups*, Adv. Math. **318** (2017), 534–626.

[5] A. Borel, *Stable real cohomology of arithmetic groups*, Ann. Sci. École Norm. Sup. (4) **7** (1974), 235–272.

[6] V. Wang. *Notes on zeta ratio stabilization*, preprint `arXiv:2402.01214` (2024).

.086... and $1 + 2 \times 10^{-7}$ (The Multiplication Table Problem)

Mehtaab Sawhney
(joint work with Ben Green)

Let

$$M(n) = |\{x \in [n] : x = x_1 x_2 \text{ with } x_i \leq n\}|.$$

The quantity $M(n)$ is exactly the number of distinct entries in the $n \times n$ multiplication table. It also arises naturally in the study of divisors of a random integer: $M(n)$ is roughly the number of integers in $[n^2]$ with a divisor in $[n/2, n]$.

Let

$$\delta = 1 - \frac{(1 + \log\log 2)}{\log 2} \approx .0860713$$

be the Erdős–Tenenbaum–Ford constant. Work of Erdős [1] proves that

$$n^2(\log n)^{-\delta+o(1)} \ll M(n) \ll n^2(\log n)^{-\delta+o(1)}.$$

This was sharpened, up to multiplicative constants, in celebrated work of Ford [5], who proved that

$$n^2(\log n)^{-\delta}(\log\log n)^{-3/2} \ll M(n) \ll n^2(\log n)^{-\delta}(\log\log n)^{-3/2}.$$

Our main theorem is the following.

Theorem 1 (Green-S. '25+)**.** *Let*

$$g(x) = \sum_{z\in\mathbb{Z}} (\log 2)^{x+z}(1 - e^{-2^{x+z}}).$$

There exist positive Borel measures μ and μ' on $\mathbb{R}/\mathbb{Z}$ such that

$$f_{\text{Mult}} = \mu * \mu' * g$$

and

$$M(n) = (1 + o_{n\to\infty}(1)) \cdot f_{\text{Mult}}\left(\left\{\frac{\log\log n}{\log 2}\right\}\right) \cdot \frac{n^2}{(\log n)^{\delta}(\log\log n)^{3/2}}.$$

There is a closely analogous statement for integers up to n with a divisor between $2^{-1}n^{1/2}$ and $n^{1/2}$. We also obtain the following corollary.

Corollary 1. *We have*

$$\frac{\max_x f_{\text{Mult}}(x)}{\min_x f_{\text{Mult}}(x)} \leq \frac{\max_x g(x)}{\min_x g(x)} < 1 + 2 \cdot 10^{-7}.$$

We conjecture that $\frac{\max_x f_{\text{Mult}}(x)}{\min_x f_{\text{Mult}}(x)} > 1$; an inequality of this type can be proved when studying divisors of smooth numbers in sufficiently short dyadic intervals.

For the purposes of exposition, we focus on a model problem for $M(n)$ given by the permutation model. Well-known results in the anatomy of integers show that, if z is not too large or too small, then the number of prime divisors between z and z^e is distributed as $\approx$ Pois(1). Thus $M(n)$ is roughly equivalent to the event of having a divisor in a specified dyadic interval. On the permutation side, for a random permutation $\sigma \in \mathfrak{S}_n$, the number of cycles with lengths between z and

ez is $\approx$ Pois(1). The question of having a divisor in a fixed dyadic interval then translates to the question of a fixed set of size k. We remark that the connection between these problems was anticipated in work of Diaconis and Soundararajan (see [4]) and the analogue of Ford's work in the permutation setting appears in Eberhard, Ford and Green [3].

For the sake of simplicity, we consider the limit $k \ll n$; in this regime we may consider a random multiset $\mathbf{A}$ in which i is included in the multiset Pois$(1/i)$ many times. Given a multiset $\mathbf{C} = \{c_1, \dots, c_\ell\}$, we set

$$\Sigma(\mathbf{C}) = \Big\{ \sum_{1 \le i \le \ell} \varepsilon_i c_i : \ \varepsilon_i \in \{0,1\} \Big\}.$$

The problem is then to understand the asymptotics of

$$p(k) = \mathbf{P}[k \in \Sigma(\mathbf{A})]$$

as $k \to \infty$; at this point the problem is purely about random sets (or multisets) of integers.

Note that

$$\mathbf{P}[k \in \Sigma(\mathbf{A})] \approx \frac{|[k] \cap \Sigma(\mathbf{A})|}{k} \ll \frac{2^{|\mathbf{A} \cap [k]|}}{k};$$

here the first approximation assumes that the event $k \in \Sigma(\mathbf{A})$ is roughly stable in dyadic ranges, while the second is the "combinatorial" bound $|\Sigma(\mathbf{C})| \le 2^{|\mathbf{C}|}$. Note that $|\mathbf{C}|$ is distributed as Pois $\big(1 + \frac{1}{2} + \cdots + \frac{1}{k}\big)$, and hence a typical sample of $\mathbf{C}$ has $\log_e k + O(1)$ elements and would therefore give a negligible contribution. The first key insight (essentially due to Erdős [1] in the number-theoretic setting) is that the dominant contribution occurs when $|\mathbf{A} \cap [k]| \approx \log_2 k$. A typical sample of $\mathbf{A}$, conditioned on this large deviation event, has $|\mathbf{A} \cap [\ell, 2\ell]|$ distributed as $\approx$ Pois(1) instead of $\approx$ Pois$(1/e)$. Working through the large deviation calculation leads to the constant δ. For the remainder of the discussion, one can in fact "change measure" and instead study $\widetilde{\mathbf{A}}$ in which i appears Pois$(1/(i \log 2))$ many times and $\widetilde{\mathbf{A}}$ has $\log_2 k + O(1)$ many elements.

The second obstruction to containing k was discovered in work of Ford [5]. Suppose that there exists m such that $|\widetilde{\mathbf{A}} \cap [k/m, k]| \le \log_2 m - \omega(1)$. Then typically

$$|\Sigma(\widetilde{\mathbf{A}} \cap [k])| \le |\Sigma(\widetilde{\mathbf{A}} \cap [k/m])| \cdot |\Sigma(\widetilde{\mathbf{A}} \cap [k/m, k])| \ll k/m \cdot 2^{\log_2 m - \omega(1)} = o(k).$$

The first bound comes from the fact that $|\Sigma(\widetilde{\mathbf{A}} \cap [k/m])|$ is bounded by the sum of elements in $\widetilde{\mathbf{A}} \cap [k/m]$ and due to the exponential spacing we typically have $|\Sigma(\widetilde{\mathbf{A}} \cap [k/m])| \ll k/m$. Therefore, for $\widetilde{\mathbf{A}}$ to contribute, we require that $|\widetilde{\mathbf{A}} \cap [k/m, k]| \ge \log_2 m - \omega(1)$ for all m. Such probabilities are closely related to the ballot theorem and play the crucial role in obtaining the $(\log\log n)^{-3/2}$ factor in the multiplication table problem.

We now conclude with a brief description of our starting point. Let $k = 2^\ell - 1$ with ℓ integral, and let $b_i = |\widetilde{\mathbf{A}} \cap [2^{i-1}, 2^i)|$ for $1 \le i \le \ell$. Rewriting the constraint

$|\widetilde{\mathbf{A}} \cap [k/m, k]| \geq \log_2 m - \omega(1)$, we obtain

$$b_1 + \ldots + b_i \leq i + \omega(1)$$

for all $1 \leq i \leq \ell$. Writing $\xi_i = b_i - 1$, we have

$$\xi_1 + \ldots + \xi_i \leq \omega(1).$$

Via a result of Ritter [2], we know that almost all such walks satisfy

$$\xi_1 + \ldots + \xi_i \leq -\min(i, \ell - i)^{1/2-\eta} + \omega(1)$$

for any fixed $\eta > 0$. Given this "parabolic" shape for the random walk, the walk naturally decomposes into three parts:

(1) large cycles,
(2) small cycles,
(3) intermediate cycles.

The measure μ arises from the large cycles, the measure μ' from the small cycles, and g from the intermediate cycles. (Ultimately we take a slowly growing $\omega(1)$ number of cycles in each of the first two classes.) Additionally, we note that μ and μ' may be given relatively explicit formulas; however, despite this description, proving that they are not uniform on $\mathbb{R}/\mathbb{Z}$ appears to be a difficult problem.

References

[1] P. Erdős, *An asymptotic inequality in the theory of numbers*, Vestnik Leningrad Univ. Mat. Mekh. i Astr., 13 (1960), pp. 41–49.
[2] G. A. Ritter, *Growth of Random Walks Conditioned to Stay Positive*, Ann. of Probab., 9 (1981), pp. 699–704.
[3] S. Eberhard, K. Ford, B. Green, *Permutations Fixing a k-Set*, International Mathematics Research Notices, Volume 2016, No. 21 (2016), pp. 6713–6736.
[4] K. Soundararajan, *Ramanujan and the anatomy of integers*, In Srinivasa Ramanujan: Going Strong at 125, Part II, *Notices Amer. Math. Soc.*, 60 (2013), no. 1, pp. 10–22.
[5] K. Ford, *The distribution of integers with a divisor in a given interval*, Ann. of Math., 168 (2008), pp. 367–433.

Prime producing sieves

Kevin Ford
(joint work with James Maynard)

We report on ongoing work to develop a general theory of prime producing sieves using Type-I and Type-II bounds which is fundamentally different than the ad-hoc, iterative methods of the Harman sieve [3]. For a very general non-negative sequence $(a_n)_{x<n\leq 2x}$ with $\sum a_n \sim x$ and "easier" comparison sequence $(b_n)_{x<n\leq 2x}$, consider the following hypotheses:

(Type-I) $$\sum_{m \leq x^\gamma} \Big| \sum_{m|n} (a_n - b_n) \Big| \ll_B \frac{x}{\log^B x},$$

(Type-II) $$\Big|\sum_{\substack{x^\theta<m\le x^{\theta+\nu}\\ x<mn\le 2x}} \xi_m\kappa_n(a_{mn}-b_{mn})\Big| \ll_B \frac{x}{\log^B x},$$

the latter holding for any divisor-bounded complex sequences ξ_m, κ_n. For example, if A is a subset of the integers in $(x, 2x]$ we can take $b_n = 1$ for all n and $a_n = \frac{x}{|A|}$ for $n \in A$, $a_n = 0$ otherwise.

Under the assumptions of the Type-I and Type-II bounds, the main questions are:

Q1. For which triples (γ, θ, ν) do we always have $\sum a_p \sim \sum b_p$?

Q2. For which triples (γ, θ, ν) do we always have $\sum a_p \gg \sum b_p$?

Here the sums are over primes p. The triples of interest are those with $\frac{1}{2} \le \gamma \le 1-\theta-\nu$ or $1-\theta \le \gamma < 1$, and either $0 \le \theta < \theta+\nu \le \frac{1}{2}$ or $0 \le \theta < \frac{1}{2}, \theta+\nu = 1-\theta$.

In a recent paper [2], we lay the foundations of our theory, completely answered Q1 and developed a toolset for answering Q2. In particular, we have

Theorem 1. *We have a guaranteed asymptotic $\sum a_p \sim \sum b_p$ if and only if both*
(A1) For all integers $n > \frac{1}{1-\gamma}$ there is an integer a with $\frac{a}{n} \in [\theta, \theta+\nu]$,
(A2) For some $h \in \mathbb{N}$, $h(1-\gamma) \in [\theta, \theta+\nu] \cup [1-\theta-\nu, 1-\theta]$.

Theorem 2. *For every $\gamma < 1$ there is a $\nu_0 > 0$ so that for any $\nu \le \nu_0$ and any θ (within the triples of interest), there is a sequence (a_n) satisfying the Type-I and Type-II bounds with $b_n = 1$ for all n, yet with $\sum_p a_p = 0$.*

The second theorem represents the first known theoretical limitations of the Type-I/Type-II sieves. In some specific cases we can say more. For example, if $\gamma = \frac{1}{2}$ and $\theta = 0$, we showed that when $\nu = \frac{1}{6}$, we always have $\sum a_p \gg \sum b_p$, while for $\nu = 0.163$, there e is a sequence (a_n) satisfying the Type-I and Type-II bounds with $b_n = 1$ for all n, yet with $\sum_p a_p = 0$.

The majority of my talk was devoted to describing our method of showing that $\sum a_p \gg \sum b_p$. At the heart is the combinatorics of two special sets of integers:

$$\mathcal{U} = \{x < n \le 2x : p|n \Rightarrow p \le x^{1-\gamma}, n \text{ has no divisor in } [x^\theta, x^{\theta+\nu}]\}$$

and $\mathcal{N}$, the set of composite $n \in (x, 2x]$ which are "coagulations" of integers $m \in \mathcal{U}$; roughly speaking, this means writing $m = d_1 \cdots d_k$ (where d_i are any integers and k is arbitrary) and replacing each d_i by a prime $p_i \asymp d_i$. We need to construct a kind of sieve weight Λ_d, supported on $d \le x^\gamma$, with $\Lambda_1 = 1$ and

$$H(n) := \sum_{d|n} \Lambda_d \le 0 \qquad (n \in \mathcal{N}).$$

This resembles a lower-bound sieve, but only restricted to $\mathcal{N}$. We show that

$$\sum (a_p - b_p) \ge \sum_{n\in\mathcal{N}} b_n H(n) + E,$$

where E is a negligible error term. The construction of good sieves Λ_d is very complicated and this is the focus of ongoing work. We are also working together with Kyle Pratt and Julia Stadlmann on constructing good sieves Λ_d for the special

1-parameter family $\gamma = \frac{3}{4} + \delta$, $\theta = \frac{1}{2} - 2\delta$, $\nu = 4\delta$, with $0 < \delta < \frac{1}{20}$. The goal here is to substantially improve the main theorem of [1].

References

[1] J. Brüdern, T. Wooley, *Partition numerorum: sums of a prime and a number of k-th powers*, J. Eur. Math. Soc. (2025), to appear.

[2] K. Ford, J. Maynard, *On the theory of prime producing sieves*, preprint `arXiv:2407.14368` (2024).

[3] G. Harman, *Prime detecting sieves*, London Mathematical Society, 2006.

On the Chowla cosine problem

Benjamin Bedert

Let $A \subset \mathbb{N}$ be a finite set of n positive integers and consider the cosine polynomial

$$f_A(x) = \sum_{a \in A} \cos ax.$$

Since $\int_0^{2\pi} f_A(x)\,dx = 0$, f_A assumes both strictly positive and strictly negative values. It is clear that $f_A(0) = n$ and $\|f_A\|_\infty = n$, so it is trivial to determine the largest positive value that f_A assumes. Determining whether f_A must assume large negative values is a hard problem; Ankeny and Chowla [10], motivated by questions on zeta functions, asked whether for any $K > 0$, there is an n_0 such that every set A of size $|A| \geq n_0$ satisfies $|\min_x f_A(x)| > K$. In 1965, Chowla [7] posed the more precise question of finding the largest number $K(n) > 0$ such that any such cosine polynomial with n terms assumes a value smaller than or equal to $-K(n)$. Chowla's cosine problem is thus to determine

$$K(n) = \min_{A \subset \mathbb{N} : |A| = n} \left(- \min_x f_A(x) \right).$$

There exist simple constructions of sets A of size n for which $\sum_{a \in A} \cos ax \geq -10\sqrt{n}$ for all x. One can for example take $A = \{b_1 - b_2 : b_j \in B\} \setminus \{0\}$ where B is a B_2-set of size $m \approx \sqrt{n}$ (and add up to $O(\sqrt{n})$ arbitrary elements if n is not of the form $m^2 - m$), and observe that $f_A = \hat{1}_A = |\hat{1}_B|^2 - |B| = |\hat{1}_B|^2 - O(\sqrt{n})$. This shows that $K(n) \ll \sqrt{n}$, which is the best known upper bound to date; in fact, Chowla [7] conjectured that this is sharp, namely that $K(n) \asymp \sqrt{n}$.

There has been gradual progress on lower bounds for Chowla's cosine problem. The first bound showing that $K(n) \to \infty$ follows from Cohen's work [4] on the Littlewood L^1 conjecture, as demonstrated by S. and M. Uchiyama [14]. This was also observed by Roth [8], who by different methods obtained the stronger bound $K(n) \gg (\log n)^c$ for $c = 1/2 - o(1)$. We note that the value of this exponent c was later improved as an immediate consequence of various papers on the L^1 conjecture, whose resolution by McGehee, Pigno and Smith [5], and independently Konyagin [6] ultimately led to $c = 1$. Bourgain [2, 3] was the first to breach the logarithmic barrier, establishing the quasipolynomial bound $K(n) > e^{(\log n)^\varepsilon}$ for some $\varepsilon > 0$. A further refinement of Bourgain's method by Ruzsa [9] shows that

$K(n) \geq e^{c'(\log n)^{1/2}}$, which stood as the record until now. We also mention that, among other results, Sanders [11] proved a polynomial bound for $|\min_x f_A(x)|$ in the special setting where all elements of A have size $O(n)$. Our main result in [1] is the following improvement, producing the first polynomial bounds for the Chowla cosine problem.

Theorem 1. *Any set $A \subset \mathbb{N}$ of $n = |A|$ positive integers satisfies*

$$\min_{x\in[0,2\pi]} \sum_{a\in A} \cos ax \leq -n^{1/7-o(1)}.$$

Hence, $K(n) \gg n^{1/7-o(1)}$. It seems likely that our method can produce an even better exponent than $1/7$, but it remains an interesting problem to investigate whether one can reach the bound $K(n) \asymp n^{1/2}$.

We remark that very recently, Jin, Milojević, Tomon and Zhang [12] independently uploaded a preprint that also establishes a polynomial bound $K(n) \gg n^c$ with the slightly weaker exponent $c = 1/10 - o(1)$. The method in our paper differs significantly from that of Jin et al., whose main theorem is a structural result about graphs with no small (i.e. large and negative) eigenvalues.

We also mention that all other methods yielding superlogarithmic bounds for $K(n)$, including those in the work [12] of Jin et al., are very sensitive to the cosine polynomials having all their coefficients in $\{0, 1\}$. Let S be a subset of $\mathbb{R} \setminus \{0\}$ and write $\mathcal{C}_S(n)$ for the class of cosine polynomials with n terms and coefficients in S. Then one can define the analogous quantity

$$K_S(n) = \min_{f\in\mathcal{C}_S(n)} \left(- \min_{x\in[0,2\pi]} f(x) \right).$$

The previous strongest general bound in the literature states that $K_S(n) \gg (\min_{s\in S} |s|) \log n$, which follows from a simple application of the L^1 conjecture (as in McGehee-Pigno-Smith [5]). Our methods provide polynomial bounds in the general setting where S is an arbitrary finite set.

Theorem 2. *Let $S \subset \mathbb{R} \setminus \{0\}$ be finite. Then there exist two constants $c_S, c'_S > 0$ such that the following holds. For every set $A \subset \mathbb{N}$ of size $n = |A|$, and every choice of coefficients $s_a \in S$, we have that*

$$\min_{x\in[0,2\pi]} \sum_{a\in A} s_a \cos(ax) \leq -c'_S n^{c_S}.$$

This result only applies when the set of coefficients S has fixed size (or sufficiently small size compared to n). One might wonder whether $K_S(n)$ exhibits polynomial growth whenever $\min_{s\in S} |s| \gg 1$, irrespective of the size of S. This is false however: a rather deep construction of Belov and Konyagin [13] shows that there exist cosine polynomials $f(x) = \sum_{j=1}^{n} a_j \cos(jx)$ with positive integer coefficients in $S = \{1, 2, \ldots, O(\log n)^3\}$ for which $\min_x f(x) \geq -O(\log n)^3$. One can alternatively interpret this as saying that the conclusion of Theorem 1 fails dramatically if one considers *multisets* $A \subset \mathbb{Z}$ of size n (whereas Chowla's cosine problem only deals with genuine sets of n distinct integers), since, instead of the

universal polynomial lower bound $-\min_x f(x) \gg n^c$, it becomes possible that $-\min_x f(x) \le (\log n)^{O(1)}$.

References

[1] B. Bedert, *Polynomial bounds for the Chowla cosine problem*, preprint `arXiv:2509.05260` (2025).

[2] J. Bourgain, *Sur le minimum d'une somme de cosinus*, Acta Arith. **45** (1986), no. 4, 381–389.

[3] J. Bourgain, *Sur le minimum de certaines sommes de cosinus*, Publ. Math. d'Orsay **84–01** (1984), No. 2, 7 pp., Univ. de Paris-Sud, Orsay.

[4] P. J. Cohen, *On a conjecture of Littlewood and idempotent measures*, Amer. J. Math. **82** (1960), no. 2, 191–212.

[5] O. C. McGehee, L. Pigno and B. Smith, *Hardy's inequality and the L^1 norm of exponential sums*, Ann. of Math. (2) **113** (1981), no. 3, 613–618.

[6] S. V. Konyagin, *On the Littlewood problem*, Izv. Akad. Nauk SSSR Ser. Mat. **45** (1981), no. 2, 243–265, 463.

[7] S. Chowla, *Some Applications of a Method of A. Selberg*, J. Reine Angew. Math. **217** (1965), 128–132.

[8] K. F. Roth, *On cosine polynomials corresponding to sets of integers*, Acta Arith. **24** (1973), no. 1, 87–98.

[9] I. Z. Ruzsa, *Negative values of cosine sums*, Acta Arith. **111** (2004), no. 2, 179–186.

[10] S. Chowla, *The Riemann zeta and allied functions*, Bull. Amer. Math. Soc. **58** (1952), no. 3, 287–305.

[11] T. Sanders, *Chowla's cosine problem*, Israel J. Math. **179** (2010), 1–28.

[12] Z. Jin, A. Milojević, I. Tomon and S. Zhang, *From small eigenvalues to large cuts, and Chowla's cosine problem*, preprint `arXiv:2509.03490` (2025).

[13] A. S. Belov and S. V. Konyagin, *An estimate for the free term of a nonnegative trigonometric polynomial with integer coefficients*, Mat. Zametki **59** (1996), no. 4, 627–629.

[14] S. Uchiyama and M. Uchiyama, *On the Cosine Problem*, Proc. Japan Acad. Ser. A Math. Sci. **36** (1960), no. 8, 475–479.

Short mollifiers of the Riemann zeta-function

Brian Conrey

(joint work with David Farmer, Kevin Kwan, Yonxiao Lin, Caroline Turnage-Butterbaugh)

There are two well-known methods for proving that a positive proportion of zeros of the Riemann zeta-function are on the critical line: Selberg's method and Levinson's method. Both methods involve mollifiers. Selberg's mollifier is the square of a smoothed Dirichlet polynomial with coefficients being those of $\zeta(s)^{-1/2}$. Levinson's mollifier is the first power of a smoothed Dirichlet polynomial with coefficients being those of $\zeta(s)^{-1}$. In both cases one works on an interval near the basic parameter T. The "length" of the mollifier is the number $\theta > 0$ where the Dirichlet polynomial is supported on $[0, T^\theta]$. In Selberg's method one may take any $\theta > 0$ and still obtain a positive proportion of zeros on the critical line. In Levinson's method it had been believed, until this work, that the mollifier must have length $\theta > 0.165$ in order to obtain a positive proportion of zeros on the critical line.

In Levinson's original paper the main calculation was the asymptotic estimate of

$$\int_0^T |\zeta(a+it) + \frac{\zeta'(a+it)}{L}|^2 |M(a+it)|^2 \, dt$$

where $L = \log T$ and

$$M(s) = \sum_{n \le y} \frac{\mu(n) \log \frac{y}{n}}{n^{1/2-a+s} \log y}$$

with $y = T^\theta$. In his thesis, Conrey showed that one may instead consider a general linear combination

$$\int_0^T \Big| Q\big(-\frac{1}{L}\frac{d}{ds}\zeta(s)\big)\Big|_{s=a+it} \Big|^2 |M(a+it)|^2 \, dt$$

where Q is a polynomial which satisfies $Q(0) = 1$ and $Q'(x) = Q'(1-x)$. His work also allowed the use of a more general mollifier

$$M(s,P) = \sum_{n \le y} \frac{\mu(n) P\big(\frac{\log \frac{y}{n}}{\log y}\big)}{n^{1/2-a+s}}$$

with $P(0) = 0$ and $P(1) = 1$. If we let κ denote the proportion of zeros of the Riemann zeta-function then the basic starting point is the theorem that

$$\kappa > \kappa(P, Q, R, \theta)$$

for any admissible P, Q, R, θ. Here $a = 1/2 - R/L$ and

$$\kappa(P, Q, R, \theta) = 1 - \frac{\log c(P, Q, R, \theta)}{R}$$

where

$$c(P, Q, R, \theta) = 1 + \frac{1}{\theta} \int_0^1 \int_0^1 \big(P'(x)w(y) + \theta P(x) w'(y)\big)^2 \, dx \, dy$$

with

$$w(y) = e^{Ry} Q(y).$$

In previous works on critical zeros, one may choose the function $P(x)$ optimally by the calculus of variations, but the function Q is chosen numerically to be a polynomial of smallish degree. Now we have determined the optimal way to choose Q, also using the calculus of variations. Remarkably, it turns out that in Levinson's method we can also take a small θ. We have proved

Theorem 1. *There is a θ_0 such that for all θ with $0 < \theta \le \theta_0$ there are choices of P, Q, R such that*

$$\kappa(P, Q, R, \theta) > \frac{2}{3}\theta.$$

The same argument applies to any primitive L-function, with the exact same form of the answer, except that the degree d of the L-function diminishes the

effective range of θ. For example, for a degree d L-function, if one can compute the relevant integral with a mollifier of length θ then one has

$$\kappa > \kappa(P, Q, R, \theta/d).$$

The effective length of the mollified is reduced by a factor of d. Thus, our result becomes especially important when dealing with families of higher degree L-functions.

We have not yet optimized all of the available parameters to obtain the optimal κ possible by Levinson's method. In particular, we don't yet know how to optimize Feng's mollifier.

References

[1] N. Andersen, J. Thorner, *Zeros of* GL_2 *L-functions on the critical line*, Forum Math. 33 (2021), no. 2, 477-491.

[2] D. Bernard, *Modular case of Levinson's theorem*, Acta Arith. 167 (2015), no. 3, 201–237.

[3] J. B. Conrey, *More than two fifths of the zeros of the Riemann zeta function are on the critical line*, J. Reine Angew. Math. 399 (1989), 1–26.

[4] S. Feng, *Zeros of the Riemann zeta function on the critical line*, J. Number Theory 132 (2012), no. 4, 511–542.

[5] N. Levinson, *More than one third of zeros of Riemann's zeta-function are on* $\sigma = 1/2$, Advances in Math. 13 (1974), 383–436.

[6] A. Selberg, *On the zeros of Riemann's zeta-function*, Skr. Norske Vid.-Akad. Oslo I (1942), no. 10, 59 pp.

3-torsion of class groups of quadratic fields

Stephanie Chan

(joint work with Peter Koymans)

Let $d \neq 1$ be a squarefree integer and let ℓ be a prime number. We denote by $h_\ell(d) := \#\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[\ell]$ the size of the ℓ-torsion subgroup of the class group, and by $h(d)$ the size of the full class group. The Brauer–Siegel theorem provides the classical bound

$$h_\ell(d) \leq h(d) \ll_\epsilon |d|^{1/2+\epsilon}.$$

This is commonly referred to as the *trivial bound* for ℓ-torsion, as it does not exploit any specific structural properties of the ℓ-torsion subgroup. Currently, no non-trivial pointwise upper bounds are known for $h_\ell(d)$ when $\ell \geq 5$. The case $\ell = 2$ goes back to Gauss, while the case $\ell = 3$ is treated in the works of Pierce [7], Helfgott–Venkatesh [4], and Ellenberg–Venkatesh [1]. The best previously known result is due to Ellenberg and Venkatesh, who proved $h_3(d) \ll_\epsilon |d|^{1/3+\epsilon}$ (see [1, Proposition 2]). In joint work with Peter Koymans, we improve this bound to

$$h_3(d) \ll_\epsilon |d|^{0.3194+\epsilon}.$$

Under standard but deep conjectures, it was previously shown that $h_3(d) \ll_\epsilon |d|^{1/4+\epsilon}$, see the works of Wong [9] and Shankar–Tsimerman [8].

Our proof strategy synthesizes techniques from several earlier works, drawing in particular on ideas from Ellenberg–Venkatesh [1], Heath-Brown–Pierce [3],

Frei–Widmer [2], Koymans–Thorner [6], and Helfgott–Venkatesh [4]. The starting point for this line of research is an observation, due independently to Michel and Soundararajan, that $h(d)/h_\ell(d)$ can be bounded below given the existence of sufficiently many small split primes. This insight was first formalized in a lemma by Ellenberg and Venkatesh in [1, Lemma 3].

To make further progress, it was soon realized that improvements to the lemma of Ellenberg–Venkatesh were essential. Allowing for more small split primes, however, comes at the cost of keeping track of the relations among them in the class group. Heath-Brown and Pierce made this explicit in the imaginary quadratic setting via a Cauchy–Schwarz type argument [3, Proposition 2.1]. Frei and Widmer treated general number fields [2, Proposition 2.1]. Koymans and Thorner [6] later combined these perspectives to produce a more flexible form of the Ellenberg–Venkatesh lemma. To obtain enough small split primes, we use a trick also due to Ellenberg–Venkatesh [1, Proposition 2], namely that the 3-rank of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-3d})$ are close by a classical reflection principle of Scholz. Looking at the splitting of primes $p \equiv 2 \bmod 3$ in the biquadratic field $\mathbb{Q}(\sqrt{d}, \sqrt{-3d})$ then implies that many small primes must split in at least one of the two fields $\mathbb{Q}(\sqrt{d})$ or $\mathbb{Q}(\sqrt{-3d})$. To control the relations among these small split primes, we return to the original argument of Helfgott and Venkatesh [4], which combines the repulsion of integral points with sphere packing techniques from [5] to give strong bounds for integral points on elliptic curves.

References

[1] J. S. Ellenberg, A. Venkatesh, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. IMRN, (1):Art. ID rnm002, 18, 2007.

[2] C. Frei, M. Widmer. *Averages and higher moments for the ℓ-torsion in class groups*, Math. Ann., 379(3-4):1205–1229, 2021.

[3] D. R. Heath-Brown, L. B. Pierce, *Averages and moments associated to class numbers of imaginary quadratic fields*, Compos. Math., 153(11):2287–2309, 2017.

[4] H. A. Helfgott, A. Venkatesh, *Integral points on elliptic curves and 3-torsion in class groups*, J. Amer. Math. Soc., 19(3):527–550, 2006.

[5] G. A. Kabatjanskii, V. I. Levenshtein, *Bounds for packings on the sphere and in space*, Problemy Peredači Informacii, 14(1):3–25, 1978.

[6] P. Koymans, J. Thorner. *Bounds for moments of ℓ-torsion in class groups*, Math. Ann., 390(2):3221–3237, 2024.

[7] L. B. Pierce, *A bound for the 3-part of class numbers of quadratic fields by means of the square sieve*, Forum Math., 18(4):677–698, 2006.

[8] A. Shankar, J. Tsimerman, *Non-trivial bounds on 2, 3, 4, and 5-torsion in class groups of number fields, conditional on standard L-function conjectures*, preprint `arXiv:2112.12949` (2023).

[9] S. Wong, *On the rank of ideal class groups*, In Number theory (Ottawa, ON, 1996), volume 19 of CRM Proc. Lecture Notes, pages 377–383. Amer. Math. Soc., Providence, RI, 1999.

Some remarks on squarefree density of polynomials

Robert C. Vaughan
(joint work with J. M. Kowalski and Yu. G. Zarhin)

The work I describe today is concerned with general integral polynomials $\mathcal{P}(\mathbf{x}) \in \mathbb{Z}[x_1, \dots, x_s]$ where for $j \le s$ we have $|x_j| \le P_j$. We extend the Möbius function by $\mu(0) = 0$. Then we define

$$N_{\mathcal{P}}(\mathbf{P}) = \sum_{\substack{\mathbf{x} \\ |x_j| \le P_j}} \mu\big(|\mathcal{P}(\mathbf{x})|\big)^2$$

and we are interested in its behaviour when $\min_j P_j \to \infty$, and the extent to which this can be approximated by

$$N_{\mathcal{P}}(\mathbf{P}) \sim 2^s P_1 \dots P_s \mathfrak{S}_{\mathcal{P}}$$

where

$$\mathfrak{S}_{\mathcal{P}} = \prod_p \left(1 - \frac{\rho_{\mathcal{P}}(p^2)}{p^{2s}}\right)$$

and

$$\rho_{\mathcal{P}}(d) = \#\{\mathbf{x} \in \mathbb{Z}_d^s : \mathcal{P}(\mathbf{x}) \equiv 0 \pmod d\}.$$

There are various general results which are dependent on unproved hypotheses and unnatural definitions of density, for example Poonen [10]. However the best general result in this direction for arbitrary degree that I am aware of is contained in Destagnol & Sofos [12]. This states that if $P_1 = \dots = P_s = P$ and $\mathcal{P} \in \mathbb{Z}[x_1, \dots, x_s]$ is separable as an element of $\mathbb{Q}[x_1, \dots, x_s]$, then

$$N_{\mathcal{P}}(\mathbf{P}) \sim 2^s P^s \mathfrak{S}_{\mathcal{P}}$$

as long as

$$s > \sigma_{\mathcal{P}} + \max\left(1, \frac{\deg(\mathcal{P}) - 1}{3}\right) 2^{\deg(\mathcal{P})}$$

and σ_f is the dimension of the singular locus of $\mathcal{P} = 0$. This depends heavily on the work of Birch [1]. For fewer variable there are a large number of special cases which have been established, beginning with Estermann [2] and Hooley [6].

The product

$$\prod_{p \le n} \left(1 - \frac{\rho_{\mathcal{P}}(p^2)}{p^{2s}}\right)$$

is a non-negative decreasing sequence so it converges as $n \to \infty$ to a non-negative limit, although when the limit is 0 it is usual to describe such a product as diverging! It seems that

$$N_{\mathcal{P}}(\mathbf{P}) \sim 2^s P_1 \dots P_s \mathfrak{S}_{\mathcal{P}}$$

should hold in all cases. Thus if $\mathcal{P}$ is such that it has a shortage of squarefree values, then we expect that

$$\mathfrak{S}_{\mathcal{P}} = 0.$$

This is easy to prove, although we have not seen it in the previous literature.

Theorem 1 (Kowalski and V. '24 [8]). *Suppose $s \geq 2$ and $\mathcal{P} \in \mathbb{Z}[x_1, \dots, x_s]$ is an integral polynomial. If $\mathfrak{S}_{\mathcal{P}} = 0$, then*

$$N_{\mathcal{P}}(\mathbf{P}) = o(P_1 \dots P_s).$$

as $\min_j P_j \to \infty$.

The proof is routine. However we can do better than this.

Theorem 2 (V. and Zharin '24 [13]). *Suppose $s \geq 1$. Then for a polynomial $\mathcal{P}$ we have*

$$\mathfrak{S}_{\mathcal{P}} = 0$$

if and only if one of the following holds.

(a) There is a prime p such that $\mathcal{P}(a_1, \dots, a_s) \in p^2\mathbb{Z}$ for all $a_1, \dots, a_s \in \mathbb{Z}$.

(b) There are polynomials $\mathcal{L}_1, \mathcal{L}_2 \in \mathbb{Z}[x_1, \dots, x_s]$ such that $\deg(\mathcal{L}_2) \geq 1$ and

$$\mathcal{P}(\mathbf{x}) = \mathcal{L}_1(\mathbf{x})\mathcal{L}_2(\mathbf{x})^2.$$

In addition, if $d = \deg(\mathcal{P})$ is odd, then $\deg(\mathcal{L}_1) \geq 1$.

As an immediate corollary we have

Corollary 1 (V. and Zharin '24 [13]). *If $\mathcal{P}$ satisfies (a), then*

$$N_{\mathcal{P}}(\mathbf{P}) = 0.$$

If it satisfies (b), then

$$N_{\mathcal{P}}(\mathbf{P}) \ll \frac{P_1 \dots P_s}{\min(P_1, \dots, P_s)}.$$

Let $\mathfrak{d}_{\mathcal{P}}$ and $\mathfrak{D}_{\mathcal{P}}$ denote the lower and upper densities

$$\mathfrak{d}_{\mathcal{P}} = \liminf_{\min\{P_1,\dots,P_s\}\to\infty} \frac{N_{\mathcal{P}}(\mathbf{P})}{2^s P_1 \dots P_s}$$

and

$$\mathfrak{D}_{\mathcal{P}} = \limsup_{\min\{P_1,\dots,P_s\}\to\infty} \frac{N_{\mathcal{P}}(\mathbf{P})}{2^s P_1 \dots P_s}$$

respectively. Then we have the following further consequence of Theorem 2

Corollary 2 (V. and Zharin '24 [13]). *We have $\mathfrak{D}_{\mathcal{P}} \leq \mathfrak{S}_{\mathcal{P}}$ and in particular if $\mathfrak{D}_{\mathcal{P}} > 0$, then $\mathfrak{S}_{\mathcal{P}} > 0$ and $\mathcal{P}$ is not of the kind described in (a) and (b) of Theorem 2.*

One can speculate as to whether it is possible to prove that $\mathfrak{d}_{\mathcal{P}} > 0$ without showing that $\mathfrak{d}_{\mathcal{P}} = \mathfrak{D}_{\mathcal{P}} = \mathfrak{S}_{\mathcal{P}} > 0$.

In a completely different direction we looked at the density of squarefree numbers in the set of numbers of the form

$$\mathcal{P}(x, y) = bx^3 + cy^k$$

where b, c are a non-zero integers and $k \geq 2$. Let θ be a constant with $0 < \theta \leq 3/k$ and suppose that X is large and Y satisfies

$$Y \asymp X^{\theta}.$$

For $h \in \mathbb{Z}$ let

$$R(h) = \#\{x, y : bx^3 + cy^k = h, |x| \le X, |y| \le Y\}.$$

Then we define

$$N_{\mathcal{P}}(X, Y) = \sum_{h \neq 0} \mu(|h|)^2 R(h)$$

and we are interested in the behaviour of this as $X \to \infty$. We expect that a good approximation for this is

$$4XY\mathfrak{S}_{\mathcal{P}}.$$

Theorem 3 (Kowalski and V. '24 [8]). *Let $\mathcal{P}$, $N_{\mathcal{P}}(X, Y)$, $\mathfrak{S}_{\mathcal{P}}$, and X, Y be as above. Suppose $(b, c) = 1$ and that $k \ge 2$. Then*

$$N_{\mathcal{P}}(X, Y) = 4XY\mathfrak{S}_{\mathcal{P}} + O\big(XY(\log X)^{-1/2}\big).$$

The cases $k = 3$ and 4 have already been treated by Filaseta [3], Greaves [5] and Sanjaya and Wang [11]. Presumably the case $k = 2$ is "well known", but is anyway covered by our result. There are two novelties in the proof.

The first is the use of the large sieve for character sums when k is not divisible by 3. The second is an estimate for the number of integer points on an elliptic curve which leads to a refinement in the use of Gallagher's larger sieve to count squares.

References

[1] B.J. Birch, *Forms in many variables*, Proc. R. Soc. Lond. Ser. A, Math. Phys. Sci. 265 (1962) 245–263.
[2] T. Estermann, *Einige Sätze über quadratfrei Zahlen*, Math. Ann. 105 (1931), 250-251.
[3] M. Filaseta, *Powerfree values of binary forms*, J. Number Theory **49** (1994), 250–268.
[4] P. X. Gallagher, *A larger sieve*, Acta Arithmetica 18(1971), 77–81.
[5] G. Greaves, *Power-free values of binary forms*, Quarterly J. Math, **43** (1992), 45–65.
[6] C. Hooley, *On the power-free values of polynomials*, Mathematika, **14** (1967), 21–26.
[7] J. M. Kowalski & R. C. Vaughan, *Squarefree density of polynomials*, Acta Arithmetica 214 (2024), 215-23.
[8] J. M. Kowalski & R. C. Vaughan, *Squarefree density of polynomials II*, Math. Annal. 391 (2024), 6037-6056.
[9] K. Lapkova & S. Y. Xiao, *Density Of Power-Free Values Of Polynomials II*, preprint `arXiv:2005.14655` (2020).
[10] B. Poonen, *Squarefree values of multivariable polynomials*, Duke Math. J., **118** (2003), 353–373.
[11] G. C. Sanjaya & X. Wang, *On the squarefree values of $a^4 + b^3$*, Math. Annalen, **386** (2023), 1237–1265.
[12] K. Destagnol & E. Sofos, *Rational points and prime values of polynomials in moderately many variables*, Bulletin des Sciences Mathématiques, **156** (2019), 1-33.
[13] R. C. Vaughan & Y. G. Zarhin, *A note on the squarefree density of polynomials*, Mathematika 70 (2024), 1-18.

L^1 means of exponential sums with multiplicative coefficients

Maksym Radziwiłł
(joint work with Mayank Pandey)

We show the following result.

Theorem 1. *Let $f : \mathbb{N} \to [-1, 1]$ be a multiplicative function such that*

$$\liminf_{N\to\infty} \frac{1}{N} \sum_{n\le N} f(n)^2 > 0.$$

If

$$\int_0^1 \Big| \sum_{n\le N} f(n)e(n\alpha)\Big| d\alpha < N^{o(1)},$$

as $N \to \infty$, then there exists a quadratic character χ such that for every $\delta > 0$, we have $|f(p) - \chi(p)| \le \delta$ for a set of primes p of logarithmic density equal to one.

The motivation for this result is two-fold. First, our result can be viewed as a "multiplicative" analogue of Littlewood's conjecture (resolved in [6, 5]) that for any sequence $a : \mathbb{N} \to \{-1, 1\}$ we have

$$\int_0^1 \Big| \sum_{n\le N} a(n)e(n\alpha)\Big| d\alpha \gg \log N. \tag{1}$$

For comparison it follows from Theorem 1 that if $f : \mathbb{N} \to \{-1, 1\}$ is multiplicative and does not pretend to be a quadratic character then there exists an $\varepsilon > 0$ such that

$$\int_0^1 \Big| \sum_{n\le N} f(n)e(n\alpha)\Big| d\alpha > N^{\varepsilon}$$

for an infinite sequence of $N \to \infty$. A slightly more technical version of our result allows one to replace "infinite sequence" by "for all".

Second, the question of lower bounds for L^1 norms of multiplicative function received attention for specific multiplicative functions [3, 1, 4, 7, 8, 9, 2]. Our result fits into this framework and is the first general result in this area.

References

[1] A. Balog, A. Perelli, *On the L^1 Mean of the Exponential Sum Formed with the Möbius Function*, Journal Of The London Mathematical Society, **57**, 275-288 (1998).
[2] A. Balog, I. A. Ruzsa, *New Lower Bound for the L^1 Mean of the Exponential Sum with the Möbius Function*, Bulletin Of The London Mathematical Society, **31**, 415-418 (1999).
[3] A. Balog, I. Ruzsa, *On the Exponential sum over r-Free Integers*, Acta Mathematica Hungarica, **90** pp. 219-230 (2001).
[4] J. Brüdern, A. Granville, A. Perelli, R. Vaughan, T. Wooley, *On the exponential sum over k-free numbers*, R. Soc. Lond. Philos. Trans. Ser. A Math. Phys. Eng. Sci., **356**, 739-761 (1998).
[5] S. Konyagin, *On the Littlewood problem*, Izv. Akad. Nauk SSSR Ser. Mat., **45**, 243-265 (1981).

[6] O. McGehee, L. Pigno, B. Smith, *Hardy's inequality and the L^1 norm of exponential sums*, Ann. Of Math.. **113** pp. 613-618 (1981).
[7] Y. Shen, *On the Balog-Ruzsa theorem in short intervals*, preprint `arXiv:2204.13531` (2022).
[8] M. Pandey, *On the distribution of additive twists of the divisor function and Hecke eigenvalues*, preprint `arXiv:2110.03202` (2021).
[9] M. Pandey, M. Radziwill, *L^1 means of exponential sums with multiplicative coefficients. I*, Compositio Math., to appear.

Erdős and $\omega(n)$

Joni Teräväinen
(joint work with Terence Tao)

Paul Erdős proved many influential results concerning the number of prime factors function $\omega(n)$. His results on the number of prime factors include the celebrated Erdős–Kac theorem on the normal distribution of $\omega(n)$ and the Erdős–Delange on the uniform distribution of $\alpha\omega(n) \pmod 1$ for α irrational.

Erdős and his collaborators also posed many problems on the distribution of $\omega(n)$. In particular, Erdős and Straus posed the following problem about long strings of consecutive values of $\omega(n)$ that we recently managed to solve.

Theorem 1. *There exists an absolute constant $C > 0$ such that for infinitely many positive integers n, for all positive integers k we have*

$$\omega(n+k) \leq \omega(n+k) \leq Ck.$$

The proof is based on the Maynard–Tao sieve method.

Another problem of Erdős in this area of study concerns the irrationality of a sum formed of $\omega(n)$. We were able to resolve this problem as well.

Theorem 2. *The series*

$$\sum_{n=1}^{\infty} \frac{\omega(n)}{2^n} = \sum_p \frac{1}{2^p - 1} = 0.5169428\ldots$$

is irrational.

The proof uses a probabilistic interpretation and an extension of a recent result of Pilatte [1] on quantitative bounds on two-point correlations of the Liouville function.

Finally, Erdős, Pomerance and Sárközy studied the problem of asymptotically counting the number of integers $n \leq x$ for which $\omega(n) = \omega(n+1)$. They obtained an upper bound of $\ll \frac{x}{\sqrt{\log\log x}}$ and conjectured that in fact this count is asymptotic to $\frac{x}{2\sqrt{\pi \log\log x}}$. We managed to confirm this conjecture for almost all x.

Theorem 3. *There is a set $\mathcal{X} \subset \mathbb{N}$ with*

$$\frac{1}{\log X} \sum_{n \in [1,X] \setminus \mathcal{X}} \frac{1}{n} \ll \log_2^{-c} X$$

for some absolute constant $c > 0$ and all sufficiently large X (so in particular, $\mathcal{X}$ has logarithmic density 1) such that for $x \in \mathcal{X}$ we have the asymptotic formula

$$\frac{1}{x}|\{n \le x : \omega(n) = \omega(n+1)\}| = \frac{1 + O(\log_2^{-c} x)}{2\sqrt{\pi \log_2 x}}$$

where $c > 0$ is an absolute constant.

The proof of this result also uses an extension of Pilatte's correlation result, along with an application of the circle method.

References

[1] C. Pilatte, *Improved bounds for the two-point logarithmic Chowla conjecture*, preprint `arXiv:2310.19357` (2023).

Manin's Conjecture for Châtelet Surfaces

Katharine Woo

Let $\Delta \in \mathbb{Q}^\times$ satisfy $\sqrt{-\Delta} \notin \mathbb{Q}$, and let $f(z) \in \mathbb{Q}[z]$ be a separable polynomial of degree 3 or 4. A Châtelet surface $X_{\Delta,f}$ over $\mathbb{Q}$ is defined as a proper smooth model of the affine surface:

$$x^2 + \Delta y^2 = f(z).$$

Châtelet surfaces appear as the simplest arithmetically nontrivial surfaces under the k-birational classification of rational surfaces – however, they can fail the Hasse principle due to the existence of Brauer-Manin obstructions. The failure of the Hasse principle for Châtelet surfaces has been classified by the seminal work of Colliot-Thélène, Sansuc and Swinnerton-Dyer [4, 5].

In this talk, we establish Manin's conjecture for Châtelet surfaces; that is, we establish an asymptotic for the number of rational points of increasing heights.

Theorem 1. *Assume that $f(z)$ decomposes into irreducible factors $f_1 \cdots f_r(z)$. Then as $B \to \infty$,*

$$\begin{aligned} N(X_{\Delta,f}, B) &:= \#\{x \in X_{\Delta,f}(\mathbb{Q}) : h(x) \le B\} \\ &\sim c_{\Delta,f} B(\log B)^{\varrho_{\Delta,f}-1} + O(B(\log B)^{\varrho_{\Delta,f}-1-10^{-10}}), \end{aligned}$$

where $\varrho_{\Delta,f}$ denotes the Picard rank

$$\varrho_{\Delta,f} = 2 + \#\{1 \le i \le r : \sqrt{-\Delta} \in \mathbb{Q}[z]/f_i(z)\},$$

and the leading constant $c_{\Delta,f} = 0$ if and only if there is a local or Brauer-Manin obstruction to the Hasse principle.

Previously, Manin's conjecture was known for all Châtelet surfaces with $\Delta = 1$ [2, 3, 6] and the techniques generalize to any positive $\Delta > 0$ generating an imaginary quadratic field of class number one. The novelty in the above result is overcoming the class number issue in the positive-definite case and handling the indefinite case (when $\Delta < 0$); this is done by bringing in the theory of automorphic forms.

The strategy to estimate $N(X_{\Delta,f}, B)$ is to first decompose the sum into an Eisenstein and cuspidal component. In the positive-definite case, this decomposition comes from writing the corresponding theta series as

$$\sum_{n=1}^{\infty} \#\{x^2 + \Delta y^2 = n\} e(nz) = E(z) + C(z),$$

where $E(z)$ is Eisenstein and $C(z)$ is cuspidal. A similar decomposition exists for the indefinite case after handling the issue of the infinite unit group of $\mathbb{Q}(\sqrt{-\Delta})$.

The estimation of the Eisenstein component follows the proof strategies of [2, 3, 6] for the case when $\Delta = 1$. The cuspidal component is bounded via two methods. The first of which uses classical facts about cusp forms and boils down to the observation that the symmetric square L-function can have, at worst, a simple pole at $s = 1$. The second method connects certain correlation sums to the base change of automorphic forms and may have applications towards other problems in analytic number theory.

Theorem 2. *Let π be a cuspidal automorphic representation of $GL_2(\mathbb{A}_{\mathbb{Q}})$ that satisfies the Ramanujan-Petersson conjecture. Let $P(x) \in \mathbb{Z}[x]$ be irreducible and solvable, and let K denote the splitting field of $P(x)$. Assume that the **base change** π_K to $GL_2(\mathbb{A}_K)$ is **cuspidal**, then the following bound holds:*

$$\sum_{n \leq X} |\lambda_\pi(|P(n)|)| \ll_{\pi,P} X \log(X)^{-0.066}.$$

References

[1] V. V. Batyrev and Y. I. Manin, *Sur le nombre des points rationnels de hauteur borné des variétés algébriques*, Math. Ann. **286** (1990), no. 1-3, 27–43.

[2] R. de la Bretèche, T. Browning and E. Peyre, *On Manin's conjecture for a family of Châtelet surfaces*, Ann. of Math. **175** (2012), no. 2, 297–343.

[3] R. de la Bretéche and G. Tenenbaum, *Sur la conjecture de Manin pour certaines surfaces de Châtelet*, J. Inst. Math. Jussieu. **12** (2013), no. 4, 759–819.

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

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

[6] K. Destagnol, *La conjecture de Manin pour certaines surfaces de Châtelet*, Acta Arith. **174** (2016), no. 1, 31–97.

[7] K. Woo, *Counting points on a family of degree one del Pezzo surfaces*, appendix on *Base change and sums of Hecke eigenvalues along polynomial sequences*, preprint `arXiv:2508.09391` (2025).

[8] K. Woo, *On Manin's conjecture for Châtelet surfaces*, preprint `arXiv:2409.17381` (2024).

Non-vanishing for cubic Hecke L-functions

Alexander Dunn

(joint work with Chantal David, Alexandre de Faveri, Joshua Stucky)

In this talk I will discuss a recent result that establishes an unconditional proportion of non-vanishing at the central point $s = 1/2$ for cubic Hecke L-functions over the Eisenstein quadratic number field. This result comes almost 25 years after Soundararajan's (2000) breakthrough result for the positive proportion of non-vanishing for primitive quadratic Dirichlet L-functions over the rational numbers.

Our proof goes through the method of first and second mollified moments. Our principal new contribution is an asymptotic evaluation of the mollified second moment with power saving error term. No asymptotic formula for the mollified second moment of a cubic family was previously known (even over function fields).

I will explain why the non-vanishing problem for cubic L-functions (via moments) has starkly different features to the corresponding problem for quadratic Dirichlet L-functions. The natural connections this problem has to cubic metaplectic forms, Gauss sums, and Heath–Brown's cubic large sieve will also be discussed.

Joint distribution for three primes

Régis de la Bretèche

The prime k-uple conjecture by Hardy and Littlewood states that for a set $\mathcal{D} := \{d_1, \dots, d_k\}$ we have

$$\sum_{1\le n\le x}\prod_{j=1}^{k}\Lambda(n+d_j) = (\mathfrak{S}(\mathcal{D})+o(1))x \qquad (x\to+\infty).$$

The term $\mathfrak{S}(\mathcal{D})$ is a singular series which satisfies

$$\mathfrak{S}(\mathcal{D}) := \prod_{p}\Big(1-\frac{1}{p}\Big)^{-k}\Big(1-\frac{\nu_p(\mathcal{D})}{p}\Big),$$

where $\nu_p(\mathcal{D})$ is the number of residue classes in $\mathcal{D}$ modulo p. Like in [7], one can prove that

$$\mathfrak{S}(\mathcal{D}) = \sum_{\substack{q_1,\dots,q_k\\ q_j\ge 1}}\Big(\prod_{j=1}^{k}\frac{\mu(q_j)}{\phi(q_j)}\Big)\sum_{\substack{a_1,\dots,a_k\\ 1\le a_j\le q_j\\ (a_j,q_j)=1\\ \sum_j a_j/q_j\in\mathbb{Z}}}\mathrm{e}\Big(\sum_{j=1}^{k}\frac{a_jd_j}{q_j}\Big),$$

where $\mathrm{e}(t) := \mathrm{e}^{2\pi it}$. Denoting $\Lambda_0 = \Lambda - 1$, the Hardy-Littlewood's conjecture can be written

$$\sum_{1\le n\le x}\prod_{j=1}^{k}\Lambda_0(n+d_j) = (\mathfrak{S}_0(\mathcal{D})+o(1))x \qquad (x\to+\infty)$$

with

$$\mathfrak{S}_0(\mathcal{D}) = \sum_{\substack{q_1,\dots,q_k\\ q_j\ge 2}} \Big(\prod_{j=1}^{k}\frac{\mu(q_j)}{\phi(q_j)}\Big) \sum_{\substack{a_1,\dots,a_k\\ 1\le a_j\le q_j\\ (a_j,q_j)=1\\ \sum_j a_j/q_j\in\mathbb{Z}}} \mathrm{e}\Big(\sum_{j=1}^{k}\frac{a_j d_j}{q_j}\Big). \tag{1}$$

Of course, the prime number theorem implies $\mathfrak{S}_0(\{d\}) = 0$ for any d. The Hardy-Littlewood's conjecture is useful to study the distribution of primes in short intervals. We have

$$\begin{aligned} M_k(X,h) &:= \frac{1}{X}\sum_{1\le n\le X}\big(\psi(n+h)-\psi(n)-h\big)^k \\ &= \frac{1}{X}\sum_{1\le n\le X}\Big(\sum_{n<m\le n+h}\Lambda_0(m)\Big)^k \\ &= \frac{1}{X}\sum_{1\le d_1,\dots,d_k\le h}\sum_{1\le n\le x}\prod_{j=1}^{k}\Lambda_0(n+d_j). \end{aligned}$$

Note that in the last sum the d_j aren't always distincts.

To be able to give an asymptotic relation for M_k we study the sum

$$R_k(h) := \sum_{\substack{d_1,\dots,d_k\\ 1\le d_j\le h\\ d_j\,\text{distinct}}} \mathfrak{S}_0(\{d_1,\dots,d_k\}).$$

In a very nice article [7], Montgomery and Soundararajan prove that

$$R_k(h) = \mu_k\big(-h\log h + Ah\big)^{k/2} + O_k\big(h^{k/2-1/(7k)+\varepsilon}\big), \tag{2}$$

where $A := 2-\gamma-\log(2\pi)$ et $\mu_k = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} x^k \mathrm{e}^{-x}\mathrm{d}x$. Moreover it is easy to prove

$$R_2(h) = -h\log h + Ah + O_k\big(h^{1/2+\varepsilon}\big).$$

When k is even, the main term of (2) comes from the contribution of terms in (1) such that $(\{a_j\}_{1\le j\le k}, \{q_j\}_{1\le j\le k})$ satisfies

$$\frac{a_j}{q_j} + \frac{a_i}{q_i} \in \mathbb{Z}$$

with $j\in J$ and $i\in I$ such that $I\sqcup J = \{1,\dots,k\}$. The number of the choice of $\{(j,i)\}$ is μ_k.

When k is odd, estimate (2) doesn't give an asymptotic relation with a main term. Lemke Oliver and Soundararajan [6] and Kuperberg [4] recently conjectured that

$$R_{2k+1}(h) \asymp h^k(\log 3h)^{k+1}.$$

Kuperberg proves in [4] that $R_3(h) \ll h(\log 3h)^5$ and Bloom and Kuperberg [1] prove that $R_{2k+1}(h) \ll h^k(\log 3h)^{C_k}$ with C_k a constant.

Our main result [2] is the estimate

$$R_3(h) = \tfrac{9}{2}h(\log h)^2\Big(1 + O\Big(\frac{(\log\log h)^{14}}{\log h}\Big)\Big) \qquad (h \geq 3). \tag{3}$$

Assuming a quantitative version of Hardy and Littlewood's conjecture on prime 3-tuples, we deduce an asymptotic formula related to the joint distribution of three primes. This improves recent results of Kuperberg and completes results by Montgomery and Soundararajan. Following the Montgomery and Soundararajan approach, we derive conjectural applications to the distribution of primes in short intervals.

The proofs are highly technical and very difficult to implement. To simplify its presentation, we see that we can parametrize q_j by

$$q_1 = gyz, \quad q_2 = gxz, \quad q_3 = gxy,$$

The condition $\sum_j a_j/q_j \in \mathbb{Z}$ is then equivalent to

$$a_1x + a_2y + a_3z \equiv 0 \pmod{gxyz}.$$

Assuming by symmetry that $x \geq y \geq z$, this is equivalent to $a_1x+a_2y \equiv 0 (\bmod z)$. One of the crucial ingredient is a nice result of Le Boudec [5] about the distribution of squarefree integers in arithmetical progression. By Hooley [3], when $(a, z) = 1$, we have

$$\sum_{\substack{1\leq n\leq X\\ n\equiv a \bmod z}} \mu(n)^2 = \frac{6X}{\pi^2 z}\prod_{p|z}(1-1/p^2)^{-1} + E(X; z, a)$$

with

$$E(X; z, a) \ll \Big(\frac{X}{z}\Big)^{1/2} + z^{1/2+\varepsilon}.$$

So for large value of z (for instance $z \geq X^{2/3}$), this doesn't give an asymptotic relation. To overcome this difficulty, we use the following result of Le Boudec

$$\sum_{\substack{1\leq a\leq z\\ (a,z)=1}} E(X; z, a)^2 \ll X(\log 2X)^5 2^{\omega(z)}.$$

As the trivial bound of this sum is X^2/z, this gives good bound when $X > zT$ with T a large parameter. The remaining case $z \leq y \leq x \leq zT$ can be bounded.

References

[1] T.F. Bloom, V. Kuperberg, *Odd moments and adding fractions*, preprint `arXiv:2312.09021` (2023).

[2] R. de la Bretèche, *Répartition conjointe de trois nombres premiers et applications*, preprint `arXiv:2410.02480` (2024).

[3] C. Hooley, *A note on square-free numbers in arithmetic progressions*, Bull. London Math. Soc. **7** (1975), 133–138.

[4] V. Kuperberg, *Odd moments in the distribution of primes*, Algebra and Number Theory (2024), to appear.

[5] P. Le Boudec, *Affine congruences and rational points on a certain cubic surface*, Algebra Number Theory **8** (2014), no. 5, 1259–1296.

[6] R.J. Lemke Oliver, K. Soundararajan, *Unexpected biases in the distribution of consecutive primes*, Proc. Natl. Acad. Sci. USA **113** (2016), no. 31, E4446–E4454.
[7] H.L. Montgomery, K. Soundararajan, *Primes in short intervals*, Comm. Math. Phys. **252** (2004), no. 1-3, 589–617.
[8] H.L. Montgomery, R.C. Vaughan, *On the distribution of reduced residues*, Ann. of Math. (2) **123** (1986), no. 2, 311–333.

Large sieve inequalities for exceptional Maass forms

Alexandru Pascadi

Several results in classical analytic number theory rely on bounds for sums of Kloosterman sums, roughly of the shape

$$\sum_{n\leq N} a_n \sum_{m\leq M} b_m \sum_{\substack{c\leq C\\(c,q)=1}} S(m\bar{q}, n; c),$$

where $M, N, C \geq 1$, $q \in \mathbb{Z}_+$, $\bar{q} \in (\mathbb{Z}/c\mathbb{Z})^\times$ denotes the inverse of q modulo c, and

$$S(m,n;c) := \sum_{x\in(\mathbb{Z}/c\mathbb{Z})^\times} e\left(\frac{mx+n\bar{x}}{c}\right).$$

In turn, bounding these exponential sums relies on the spectral theory of GL_2 automorphic forms of level q, and in particular on large sieve inequalities for their Fourier coefficients. The dominant contribution in these estimates often comes from the 'exceptional' Maass cusp forms f, which are eigenforms of the hyperbolic Laplacian with eigenvalues $\lambda_f < \frac{1}{4}$. Selberg's eigenvalue conjecture asserts that these forms do not exist, but unconditionally they may produce substantial losses of the form X^{θ_f}, where X is a large parameter and

$$\theta_f := \sqrt{\max\left(0, \frac{1}{4} - \lambda_f\right)}$$

measures the extent to which Selberg's conjecture fails. To counter these potential losses in the exceptional spectrum, one can rely on on-average substitutes for Selberg's conjecture. The resulting large sieve inequalities have the shape

$$\sum_{\lambda_f<\frac{1}{4}}^{\Gamma_0(q)} X^{2\theta_f} \left|\sum_{N<n\leq 2N} a_n \rho_f(n)\right|^2 \ll (Nq)^{o(1)} \left(1+\frac{N}{q}\right) \|a\|_2^2, \tag{1}$$

where the sum is over an orthonormal basis of exceptional Maass forms f for $\Gamma_0(q)$, $\rho_f(n)$ are their Fourier coefficients (typically of size $\approx q^{-1/2}$) around ∞ (or another fixed cusp of $\Gamma_0(q)$), $(a_n)_{N<n\leq 2N}$ is a complex sequence, $\|a\|_2^2 := \sum_n |a_n|_2^2$, and $X = X(q, N, (a_n)_{N<n\leq 2N}) > 0$. Note that X only appears in the left-hand side, and that the right-hand side matches the bound for the regular-spectrum forms f with $\lambda_f \ll 1$. Results like (1) achieve two effects at once:

(*i*). A strong orthogonality property of the Fourier coefficients $\rho_f(n)$, akin to more classical large sieve inequalities;

(*ii*). A saving of $X^{2\theta_{\max}}$ in the exceptional-eigenvalue aspect, where $\theta_{\max} := \sup_{\lambda_f<1/4} \theta_f \leq \frac{7}{64}$ (the pointwise bound is due to Kim–Sarnak [5]).

The goal is then to maximize X in terms of q, N, and the sequence $(a_n)_{N<n\leq 2N}$. The first such large sieve inequality is due to Deshouillers–Iwaniec [2, Theorems 2 and 5], who proved the following.

Theorem 1 (Deshouillers-Iwaniec '82 [2]). *The bound* (1) *holds for any complex sequence* $(a_n)_{N<n\leq 2N}$ *and*

$$X = \max\left(1, \frac{q}{N}\right).$$

Theorem 1 is actually optimal for general sequences $(a_n)_{N<n\leq 2N}$. Our first key observation is that in many applications, the sequences $(a_n)_{N<n\leq 2N}$ have a special 'additive' structure, in the sense that their Fourier transforms are supported on sparse subsets of $\mathbb{R}/\mathbb{Z}$. This raises the possibility of saving more in the X^θ-aspect.

In [9], we prove better large sieve inequalities for exceptional Maass forms for additively-structured sequences $(a_n)_{N<n\leq 2N}$. It is easiest to state here the particular case when a_n is given by a simple exponential phase.

Theorem 2 (P. '24+ [9]). *For any* $\alpha \in \mathbb{R}/\mathbb{Z}$, *the bound* (1) *holds with* $a_n = e(n\alpha)$ *and*

$$X = \max\left(\sqrt{N}, \frac{q}{\sqrt{N}}\right).$$

In fact, we can accommodate larger values of X, up to $\max(N, q)$, depending on the quality of rational approximations to α. Our proof uses the Kuznetsov trace formula and Fourier analysis, followed by (a slight extension) of an argument of Cilleruelo–Garaev [1] for counting points on a modular hyperbola.

Theorem 2 has applications to the exponents of distribution of primes and smooth numbers in arithmetic progressions to large moduli.

Theorem 3 (P. '25+ [10]). *The primes have exponent of distribution* $5/8 - o(1)$ *in arithmetic progressions, using triply-well-factorable weights for the moduli.*

Theorem 4 (P. '25+ [10]). *The* $x^{o(1)}$*-smooth numbers up to* x *have exponent of distribution* $5/8 - o(1)$ *in arithmetic progressions, using arbitrary* 1*-bounded weights for the moduli.*

Both Theorems 3 and 4 improve on the previous exponent of $66/107 - o(1)$ due to Lichtman [6] and Pascadi [11], which improved in turn on the exponent of $3/5 - o(1)$ due to Maynard [7] and Drappeau [3]. They also imply sharper upper bounds for the number of twin primes and consecutive smooth numbers up to x [10]. The key qualitative feature of these results is that they are as good as assuming Selberg's eigenvalue conjecture.

We also mention the following independent application.

Theorem 5 (P. '24+ [9]). *The greatest prime factor of* $n^2 + 1$ *is infinitely often greater than* $n^{1.3}$.

The threshold of $n^{1.3}$ in Theorem 5 improved on Merikoski's $n^{1.279}$ [8], by partially removing the dependency on progress towards Selberg's eigenvalue conjecture. It was recently further improved to $n^{1.312}$ by Grimmelt–Merikoski [4], who completely removed this dependency.

References

[1] J. Cilleruelo Mateo and M. Z. Garaev, *Concentration of points on two and three dimensional modular hyperbolas and applications*, Geom. Funct. Anal. **21** (2011), no. 4, 892–904; MR2827013

[2] J.-M. Deshouillers and H. Iwaniec, *Kloosterman sums and Fourier coefficients of cusp forms*, Invent. Math. **70** (1982/83), no. 2, 219–288.

[3] S. Drappeau, *Théorèmes de type Fouvry-Iwaniec pour les entiers friables*, Compos. Math. **151** (2015), no. 5, 828–862.

[4] L. Grimmelt, J. Merikoski, *On the greatest prime factor and uniform equidistribution of quadratic polynomials*, preprint `arXiv:2505.00493` (2025).

[5] H. H. Kim, *Functoriality for the exterior square of* GL_4 *and the symmetric fourth of* GL_2, J. Amer. Math. Soc. **16** (2003), no. 1, 139–183. Appendix 2 by H. H. Kim and P. Sarnak.

[6] J. D. Lichtman, *Primes in arithmetic progressions to large moduli, and Goldbach beyond the square-root barrier*, preprint `arXiv:2309.08522` (2023).

[7] J. A. Maynard, *Primes in arithmetic progressions to large moduli II: Well-factorable estimates*, Mem. Amer. Math. Soc. **306** (2025), no. 1543, v+33 pp.

[8] J. Merikoski, *On the largest prime factor of* n^2+1, J. Eur. Math. Soc. **25** (2023), no. 4, 1253–1284.

[9] A. Pascadi, *Large sieve inequalities for exceptional Maass forms and the greatest prime factor of* n^2+1, preprint `arXiv:2407.14368` (2024).

[10] A. Pascadi, *On the exponents of distribution of primes and smooth numbers*, preprint `arXiv:2505.00653` (2025).

[11] A. Pascadi, *Smooth numbers in arithmetic progressions to large moduli*, Compos. Math. **161** (2025), no. 8, 1923–1974.

Erdős's integer dilation approximation problem

Dimitris Koukoulopoulos

(joint work with Youness Lamzouri and Jared Duker Lichtman)

Given a set of real numbers $\mathcal{A} \subset \mathbb{R}_{>0}$ and $\varepsilon > 0$, Erdős [4] proposed the following Diophantine problem: is it possible to find a pair of distinct elements $\alpha, \beta \in \mathcal{A}$ and an integer n such that

$$|n\alpha - \beta| < \varepsilon\,? \tag{1}$$

Note that this is trivially true if the distances between different elements of $\mathcal{A}$ become arbitrarily small. We will thus be assuming from now on that $\mathcal{A}$ is *well-spaced*, meaning that there exists a constant $c > 0$ such that $|\alpha - \beta| \geq c$ for all pairs (α, β) of distinct elements of $\mathcal{A}$. In particular, $\mathcal{A}$ will be a countable set.

In 1948, Erdős [4, Page 692] asked whether it is possible to find solutions to (1) if $\mathcal{A}$ is "large enough". Motivated by his work [3] and that of Behrend [2] on integer primitive sequences (see Definition 1 below and the discussion following it),

he proposed that this might indeed be possible if $\mathcal{A}$ satisfies one of the following conditions:

$$\sum_{\alpha\in\mathcal{A},\,\alpha\geq 2}\frac{1}{\alpha\log\alpha}=\infty \tag{2}$$

or

$$\limsup_{x\to\infty}\frac{1}{\log x}\sum_{\alpha\in\mathcal{A}\cap[1,x]}\frac{1}{\alpha}>0. \tag{3}$$

We shall refer to this question as the *integer dilation approximation problem*. This problem was mentioned[1] again in [5, 6, 7, 8, 9, 10, 11, 12, 13, 14].

In [18], we resolved Erdős's integer dilation approximation problem when $\mathcal{A}$ satisfies the second condition (3).

Theorem 1. *Let $\mathcal{A}\subset\mathbb{R}_{>0}$ be a countable set such that*

$$\limsup_{x\to\infty}\frac{1}{\log x}\sum_{\alpha\in\mathcal{A}\cap[1,x]}\frac{1}{\alpha}>0.$$

Then, for every $\varepsilon>0$, there exists a pair $(\alpha,\beta)\in\mathcal{A}^2$ such that $\alpha\neq\beta$ and $|n\alpha-\beta|<\varepsilon$ for some positive integer n.

It is worth noting that Erdős originally stated his problem in its contrapositive form; the above formulation of the problem appeared first in a paper of Erdős and Sárközy [13], and subsequently in Haight's 1988 work [16], who proved Theorem 1 in the special case when the ratios α/β with distinct $\alpha,\beta\in\mathcal{A}$ are all irrational. As a matter of fact, under this assumption, Haight proved the stronger estimate

$$\lim_{x\to\infty}\frac{1}{x}\sum_{a\in\mathcal{A}\cap[1,x]}1=0.$$

Erdős's motivation for stating the problem in the contrapositive form comes from its connection to *primitive sets* of integers. Indeed, if $\mathcal{A}\subset\mathbb{N}$ and $\varepsilon\in(0,1]$, then the only way to have a solution to (1) is if $\beta=n\alpha$, that is to say, if α divides β. Let us now recall the definition of a primitive set:

Definition 1 (Primitive set)**.** *We say that a set $\mathcal{A}\subset\mathbb{N}$ is primitive if $a\nmid b$ for all distinct $a,b\in\mathcal{A}$.*

If $\mathcal{A}$ is a primitive set of integers, Erdős [3] proved that

$$\sum_{a\in\mathcal{A},\ a>1}\frac{1}{a\log a}<\infty,$$

while Behrend proved [2] proved that

$$\sum_{a\in\mathcal{A}\cap[1,x]}\frac{1}{a}\ll\frac{\log x}{\sqrt{\log\log x}}, \tag{4}$$

[1] In [12], which was published in 1997, shortly after Paul Erdős passed away, he wrote "I offer \$500 for settling this annoying diophantine problem."

The connection of Erdős's problem to primitive sets of integers plays a crucial role in our proof, as does Haight's work. In fact, one may view our proof as an instance of the *structure versus randomness* philosophy.

Let us consider a countable set $\mathcal{A} \subset \mathbb{R}_{\geq 1}$ and a number $\varepsilon \in (0, 1]$ such that there are no solutions to the inequality $|n\alpha - \beta| < \varepsilon$ with distinct $\alpha, \beta \in \mathcal{A}$ and with $n \in \mathbb{N}$. In order to establish Theorem 1, we must prove that

$$\sum_{\alpha \in \mathcal{A} \cap [1,x]} \frac{1}{\alpha} = o(\log x) \quad (x \to \infty). \tag{5}$$

We have two extreme cases:

- *Structured sets:* these are primitive sets or small "perturbations" of them. By this, we mean that $\mathcal{A} \subseteq \gamma \mathbb{Q}_{\geq 1} := \{\gamma\rho : \rho \in \mathbb{Q}_{\geq 1}\}$ for some $\gamma \in \mathbb{R}_{\geq 1}$, and that the set of denominators
$$\mathcal{Q} = \big\{q \in \mathbb{N} : \exists a \in \mathbb{N} \text{ such that } \gcd(a, q) = 1 \text{ and } \gamma a/q \in \mathcal{A}\big\}$$
is sparse. For each given $q \in \mathcal{Q}$, the set $\{a \in \mathbb{N} : \gcd(a, q) = 1,\ a/q \in \mathcal{A}\}$ is primitive, so we may apply Behrend's estimate (4) to it (more precisely, we need its strengthening by Ahlswede, Khachatrian and Sárközy [1].) If $\mathcal{Q}$ is sparse enough, then we deduce that (5) holds.
- *Random sets:* these are sets $\mathcal{A}$ for which all ratios α/β are irrational, or perhaps rational numbers of large height. We can expect to be able to handle such sets by a suitable variant of Haight's proof and to prove that (5) holds for them too.

Roughly speaking, the strategy of the proof is to show that either $\mathcal{A}$ consists almost 100% of a random set, or that a positive proportion of $\mathcal{A}$ is structured.

In order to extract the needed structure, we adapt the machinery of GCD graphs developed jointly with James Maynard in the proof of the Duffin–Schaeffer conjecture [19]. Moreover, we need some important technical ideas introduced by Green–Walker [15] and developed further by Hauke–Vazquez–Walker [17].

References

[1] R. Ahlswede, L. Khachatrian, A. Sárközy, *On the density of primitive sets*, J. Number Theory, (2004), 319–361.

[2] F. Behrend, *On sequences of numbers not divisible by another*, J. Lond. Math. Soc. (1935), 42–45.

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

[4] ———, *On the density of some sequences of integers*, Bull. Amer. Math. Soc. 54 (1948), 685–692.

[5] ———, *Some unsolved problems.* Magyar Tud. Akad. Mat. Kutató Int. Közl, (1961), 221–254.

[6] ———, *Quelques problèmes de théorie des nombres*, Monographies de l'Enseignement Mathématique, No. 6 , pp. 81–135, L'Enseignement Mathématique, Université, Geneva, 1963.

[7] ———, *Problems and results on combinatorial number theory.* A survey of combinatorial theory (Proc. Internat. Sympos., Colorado State Univ., Fort Collins, Colo., 1971), pp. 117–138. North-Holland Publishing Co., Amsterdam-London, 1973.

[8] ———, *Problems and results on Diophantine approximations, II.* Lecture Notes in Math., 475, pp. 89–99, Springer, Berlin, 1975.
[9] ———, *Problèmes extrémaux et combinatoires en théorie des nombres*, Séminaire Delange-Pisot-Poitou (17e année: 1975/76), Théorie des nombres, Fasc. 2, Exp. No. 67 , 5 pp., Secrétariat Mathématique, Paris, 1977.
[10] ———, *A survey of problems in combinatorial number theory, Combinatorial mathematics, optimal designs and their applications*, Ann. Discrete Mathematics 6 (1980), 89–115.
[11] ———, *Some of my forgotten problems in number theory*, Hardy-Ramanujan J. 15 (1992), 34–50.
[12] ———, *Some of my favorite problems and results*, The mathematics of Paul Erdős, I, 47–67, Algorithms Combin., 13, Springer-Verlag, Berlin, 1997.
[13] P. Erdős and A. Sárközy, *Some solved and unsolved problems in combinatorial number theory*, Math. Slovaca 28 (1978) no. 4, 407–421
[14] P. Erdős, A. Sárközi and E. Szemerédi, *On divisibility properties of sequences of integers*, Colloq. Math. Soc. János Bolyai, 2 North-Holland Publishing Co., Amsterdam-London, 1968, pp. 35–49.
[15] B. Green and A. Walker, *Extremal problems for GCDs*, Combin. Probab. Comput. 30 (2021), no. 6, 922–929.
[16] A. J. Haight, *On multiples of certain real sequences*, Acta Arith. 49 (1988), no. 3, 303–306.
[17] M. Hauke, S. Vazquez Saez and A. Walker, *Proving the Duffin-Schaeffer conjecture without GCD graphs*, preprint `arXiv:2404.15123` (2024).
[18] D. Koukoulopoulos, Y. Lamzouri and J. D. Lichtman, *Erdős's integer dilation approximation problem and GCD graphs*, preprint `arXiv:2502.09539` (2025).
[19] D. Koukoulopoulos and J. Maynard, *On the Duffin-Schaeffer conjecture.* Ann. of Math. (2) 192 (2020), no. 1, 251–307.

An inverse theorem for the Gowers U^3-norm relative to quadratic level sets

Sean Prendiville

Gowers uniformity norms have become well-used tools in the (higher-order) circle method, allowing one to count certain arithmetic configurations of interest - configurations out of reach of the classical circle method. For instance, within the prime numbers, the count of four-term arithmetic progressions is intimately connected with the U^3-norm of the von Mangoldt function [1].

Central to the utility of these uniformity norms are so-called inverse theorems, which characterise when they are large. When a function is defined on a finite vector space $\mathbb{F}_p^n$, the inverse theorem says that the U^3-norm is large only if the function correlates with a quadratic phase,

$$x \mapsto e^{2\pi i q(x)/p},$$

where $q : \mathbb{F}_p^n \to \mathbb{F}_p$ is a quadratic polynomial [2]. This is a useful global characterisation of when the U^3-norm is large. It allows one to account for all the quadratic phases which lead to a function having a large U^3-norm. Using an arithmetic regularity lemma, one can decompose a function into a main term, consisting of a linear combination of a small number of quadratic phases, and an error term which has a small U^3-norm. This reduces the task of counting (say) four-term arithmetic

progressions along a function, to the task of counting four-term progressions along quadratic phases.

There are situations in arithmetic combinatorics where it is quantitatively inefficient to try and account for all the possible global behaviour of a function — there are too many quadratic phases to account for. It is therefore more efficient to localise, as one has to account for less behaviour locally. For such purposes, one needs an analogue of the inverse theorem for the Gowers U^3-norm, but where the function has support contained in a sparse set of the ambient vector space $\mathbb{F}_p^n$. It turns out that, for the U^3-norm, the appropriate set on which to localise is the zero locus on a collection of quadratic polynomials (a quadratic level set).

We discuss an effective inverse theorem for the Gowers U^3-norm, localised to quadratic level sets. This enables one to perform the (quadratic) circle method locally, and thereby improve error terms when counting. We discuss the benefit of localising in additive combinatorics, improving a bound on the Ramsey number of three-term progressions which are the same colour as their common difference ("Brauer quadruples"), a result it seems difficult to obtain by other means.

References

[1] Ben Green, *Generalising the Hardy-Littlewood method for primes*, International Congress of Mathematicians, Vol. II, 373–399, European Mathematical Society (EMS), Zürich, 2006.

[2] Ben Green and Terence Tao, *An inverse theorem for the Gowers $U^3(G)$ norm*, Proc. Edinb. Math. Soc. (2) 51 (2008), no. 1, 73–153.

[3] S. Prendiville, *An inverse theorem for the Gowers U^3-norm relative to quadratic level sets*, preprint `arXiv:2409.07962` (2024).

Shifted convolution sums and L-functions

Junxian Li

(joint work with Valentin Blomer)

A shifted convolution problem asks for an asymptotic formula for

$$\sum_{n\leq x} a(n)b(n+1) \tag{1}$$

where $a(n)$ and $b(n)$ are two arithmetic functions, usually of multiplicative nature. The shifted convolution problem is not only interesting on its own, such as the twin prime conjecture and the Chowla conjecture, but is also closely related to problems on moments of L-functions, the subconvexity problem as well as the quantum unique ergodicity conjecture.

Shifted convolutions sums on Fourier coefficients of $GL(2)$ automorphic forms have been extensively studied in the past century, yet shifted convolution problems with Fourier coefficients of higher rank automorphic forms turn out to be extremely challanging, and non-trivial results are unknown in most cases. Progress has been made when one factor is associated with an automorphic form on GL(3) and the

other is associated with an automorphic form on GL(2). The asymptotic formula for the most factorable case

$$\sum_{n\leq x}\tau_3(n)\tau(n+1), \tag{2}$$

where $\tau_3 = \mathbf{1} * \mathbf{1} * \mathbf{1}$ denotes the ternary divisor function, was first obtained by Hooley [Ho] and a power saving error term was first made by Deshouillers [De] using the Kuznetsov formula. The current record is due to Topacogullari [To]. In the case when the divisor function τ in (2) is replaced with a GL(2) Fourier coefficient, i.e.

$$\sum_{n\leq x}\tau_3(n)\lambda(n+1), \tag{3}$$

Pitt [Pi1] first established a power saving bound for (3), which is an important ingredient in his cuspidal version of the Titchmarsh divisor problem [Pi2]. The current record is due to H. Tang [Ta]. The convolution structure of $\tau_3 = \mathbf{1} * \mathbf{1} * \mathbf{1}$ was crutially used in both of these two results. It was Munshi who first established the case where both factors in (2) are cuspidal, i.e.

$$\sum_{n\leq x}A(n,1)\lambda(n+1) \tag{4}$$

for a GL(3) Fourier coefficient $A(n,1)$ and a GL(2) Fourier coefficient $\lambda(n)$. The current record is due to P. Xi [Xi]. Munshi's proof of (4) uses Jutila's version of the circle method where factorizable moduli were empolyed to create a bilinear structure. However, Jutila's circle method is only (directly) applicable if general exponential sums in at least one of the involved arithmetic functions have uniform square-root cancellation. This is not true for the divisor function and is not known for GL(3) Hecke eigenvalues. In particular, the last remaining case where $\lambda(n)$ is replaced by $\tau(n)$ in (4) remained open and cannot be attacked by any of the methods used to treat (2), (3) or (4). Note that if we expand the divisor function τ and apply the Voronoi summation formula, then we would encouter a sum of hyper-Kloosterman sums twisted by $GL(3)$ Fourier coefficients, where non-trivial estimate over the moduli is not available.

In this paper we overcome these difficulties and establish the remaining case for $GL(3)\times GL(2)$ shifted convolution sums with a more general shift condition and complete uniformity by developing a new version of the delta symbol method.

Theorem 1. *Let $h,\lambda_1,\lambda_2\in\mathbb{Z}\setminus\{0\}$, $x\geq 1$. Let W, W_0 be smooth functions with compact support in $[1,2]$. Let $A(n,1)$ denote the Hecke eigenvalues of a cusp form F for the group $\mathrm{SL}_3(\mathbb{Z})$. Then*

$$\sum_{\lambda_1 m-\lambda_2 n=h}A(n,1)\tau(m)W_0\Big(\frac{|\lambda_1|m}{x}\Big)W\Big(\frac{|\lambda_2|n}{x}\Big)\ll_{F,W,W_0,\varepsilon}x^{41/42+\varepsilon}$$

for any $\varepsilon>0$, uniformly in h,λ_1,λ_2.

The proof of Theorem 1 combines for the first time two different delta symbol methods – Jutila's method and a modern version of the Kloosterman method –

that are applied in an intertwined fashion. Our new version of the delta symbol gives the flexibility to choose moduli in a way that creates a bilinear structure for the minor arcs, and at the same time allows a Kloosterman refinement on the major arcs, i.e. a non-trivial (and in fact square-root saving) estimate over the fractions b/c for b modulo c.

The proof in Theorem 1 can be used to establish an asymptotic formula for a twisted moment of L-functions on GL(3).

Theorem 2. *Let $Q \geq 1$ and let F be a cusp form for the group $\mathrm{SL}_3(\mathbb{Z})$. Let W be a smooth function with compact support in $[1,2]$ and Mellin transform $\widetilde{W}$. Then*

$$\sum_q W\Big(\frac{q}{Q}\Big) \sum_{\substack{\chi \,(\mathrm{mod}\ q)\\ \chi \text{ primitive, even}}} L(1/2, F\times\chi) = \frac{\widetilde{W}(2)}{2\zeta(2)^2}Q^2 + O_{F,W,\varepsilon}(Q^{2-1/41+\varepsilon})$$

for any $\varepsilon > 0$.

Theorem 2 features a moment containing roughly Q^2 terms for an L-function of conductor roughly Q^3. Nevertheless, up until now, only an asymptotic formula over a subsequence of moduli q was available by Luo [Lu], which was a hard-earned result and is now over 20 years old. Since the central values $L(1/2, F\times\chi)$ are not non-negative, Luo's result gives neither a lower nor an upper bound for the moment considered in Theorem 2. Luo's result [Lu] also used crucially the idea of factorizable moduli, as in Munshi [Mu]. As in Theorem 1, Theorem 2 would be straightforward if non-trivial averages of hyper-Kloosterman sums over the moduli were available.

References

[De] J.-M. Deshouillers, *Majorations en moyenne de sommes de Kloosterman,* Université de Bordeaux I, Laboratoire de Théorie des Nombres, Talence, 1982, Exp. No. 3, 5 pp.

[Ho] C. Hooley, *An asymptotic formula in the theory of numbers*, Proc. London Math. Soc. **7** (1957), 396–413.

[Lu] W. Luo, *Nonvanishing of L-functions for* $\mathrm{GL}(n, \mathbb{A}_{\mathbb{Q}})$, Duke Math. J. **128** (2005), 199–207.

[Mu] R. Munshi, *Shifted convolution sums for* $\mathrm{GL}(3)\times\mathrm{GL}(2)$, Duke Math. J. **162** (2013), 2345–2362.

[Pi1] N. Pitt, *On shifted convolutions of $\zeta_3(s)$ with automorphic L-functions*, Duke Math. J. **77** (1995), 383–406.

[Pi2] N. Pitt, *On an analogue of Titchmarsh's divisor problem for holomorphic cusp forms,* J. Amer. Math. Soc. **26** (2013), 735–776.

[Ta] H. Tang, *A shifted convolution sum of d_3 and the Fourier coefficients of Hecke-Maass forms II,* Bull. Aust. Math. Soc. **101** (2020), 401–414.

[To] B. Topacogullari, *The shifted convolution of divisor functions*, Q. J. Math. **67** (2016), 331–363.

[Xi] P. Xi, *A shifted convolution sum for* $\mathrm{GL}(3)\times\mathrm{GL}(2)$, Forum Math. **30** (2018), 1013–1027.

Primes of the form $p^2 + nq^2$

Ben Green
(joint work with Mehtaab Sawhney)

Overview. The study of primes of the form $x^2 + ny^2$ is a very classical topic. For example, Weber proved in 1882 that for any $n \geq 1$ there exist infinitely many primes of the form $x^2 + ny^2$.

More recent work poses additional restrictions on the variables x and y. In the case $n = 1$, Fouvry and Iwaniec [2] showed that there are infinitely many primes of the form $x^2 + y^2$ with x prime, while Friedlander and Iwaniec [3] famously showed that one may insist that x is a square. Heath–Brown and Li [5] refined this result, showing that one may ask that x be the square of a prime. More recently Merikoski [9] showed that one may restrict x to any sufficiently dense set S satisfying a condition such as $|S \cap [N]| \geq N^{1-\delta}$ for all N.

Placing constraints on both x and y is (even) more difficult. In this direction, Friedlander and Iwaniec [4] showed that there are infinitely many triples with x prime, y having at most seven prime factors, and $x^2 + 4y^2$ itself prime. They conjectured that one may insist that y is also prime.

Main Theorem. In work with M. Sawhney we resolve this conjecture of Friedlander and Iwaniec, and in fact prove the following more general result.

Theorem 1. *For $n \equiv 0$ or $4 \pmod 6$, there exist infinitely many primes of the form $x^2 + ny^2$ with both x and y prime.*

Moreover, we have the following asymptotic formula for any $W \in C_0^\infty(\mathbb{R})$:

$$\sum_{x,y\in\mathbb{Z}} \Lambda(x)\Lambda(y)\Lambda(x^2+ny^2)W\Big(\frac{x}{N},\frac{y}{N}\Big) = \kappa_n N^2 \int_{\mathbb{R}^2} W + O_W\left(\frac{N^2(\log\log N)^2}{\log N}\right),$$

where

$$\kappa_n = \lim_{X\to\infty} \prod_{\substack{p\leq X\\(-n|p)=1}} \frac{p(p-3)}{(p-1)^2} \prod_{\substack{p\leq X\\(-n|p)\neq 1}} \frac{p}{(p-1)}.$$

The Euler product converges conditionally and can be rearranged (using the class number formula) so as to converge absolutely.

Sums over Gaussian primes. For brevity we discuss the argument in the case $n = 4$. It is natural to work in the Gaussian integers $\mathbb{Z}[i]$, since $x^2 + 4y^2 = N_{\mathbb{Q}[i]/\mathbb{Q}}(x + 2iy)$. This essentially reduces matters to obtaining an asymptotic for the sum

$$\sum_{\substack{N(\alpha)\leq X\\ \alpha \text{ prime}}} F(\alpha), \qquad F(x+2iy) = \Lambda(x)\Lambda(y),$$

where α ranges over primes in $\mathbb{Z}[i]$.

To control such sums, one uses the method of bilinear forms, also known as the method of Type I/II sums. We use a particular instance of this due to Duke–Friedlander–Iwaniec [1], which allows one to control sums over primes given Type I estimates up to $X^{1/2}$ and Type II estimates to $X^{1/3}$.

Decomposition of von Mangoldt. We do not address the above sum directly using the method of bilinear forms, but first decompose

$$\Lambda = \Lambda^\sharp + f, \quad \text{where} \quad \Lambda^\sharp(x) = \prod_{p \le Q} (1 - 1/p)^{-1} 1_{(x,p)=1}$$

is a smooth Cramér-type approximant. The main term in our asymptotic arises from $\Lambda^\sharp(x)\Lambda^\sharp(y)$, while the error contributions involving $f = \Lambda - \Lambda^\sharp$ are shown to be small using Type I/II estimates.

A key step is to prove that the "product weight"

$$w(x + 2iy) = f(x)f(y)$$

satisfies the necessary Type I and II bounds.

The main new ideas in the paper lie in the treatment of the Type II bounds, and here we use the theory of *Gowers uniformity norms* from additive combinatorics. One shows that a (putative) large Type II sum implies a large Gowers uniformity norm $\|f\|_{U^k}$ for appropriate k. For the specific function $f = \Lambda - \Lambda^\sharp$ this can then be ruled out using recent work of Leng [7] and Leng–Sah–Sawhney [8].

The proof of this key proposition uses the machinery of *concatenation*, and in particular work of Borys Kuca [6]. After some initial Cauchy–Schwarz manipulations of standard type (analogous to the analysis of 4-term arithmetic progressions via the U^3-norm), one controls f via a certain average of so-called *Gowers–Peluse norms*, which are analogues of Gowers uniformity norms in which the difference variables are restricted. The machinery of concatenation then allows us to upgrade such local control to a global bound on the Gowers norm.

References

[1] W. Duke, J. Friedlander and H. Iwaniec, *Equidistribution of roots of a quadratic congruence to prime moduli,* Ann. of Math. (2) **141** (1995), no. 2, 423–441.

[2] E. Fouvry and H. Iwaniec, *Gaussian primes,* Acta Arith. **79** (1997), no. 3, 249–287.

[3] J. Friedlander and H. Iwaniec, *The polynomial $X^2 + Y^4$ captures its primes,* Ann. of Math. (2) **148** (1998), no. 3, 945–1040.

[4] J. Friedlander and H. Iwaniec, *Coordinate distribution of Gaussian primes,* J. Eur. Math. Soc. (JEMS) **24** (2022), no. 3, 737–772.

[5] D. R. Heath-Brown and X. Li, *Prime values of $a^2 + p^4$*, Invent. Math. **208** (2017), no. 2, 441–499.

[6] B. Kuca, *Multidimensional polynomial patterns over finite fields: bounds, counting estimates and Gowers norm control,* Adv. Math. **448** (2024), Paper No. 109700, 61 pp.

[7] J. Leng, *Efficient Equidistribution of Nilsequences*, preprint `arXiv:2312.10772` (2024).

[8] J. Leng, A. Sah, and M. Sawhney, *Quasipolynomial bounds on the inverse theorem for the Gowers $U^{s+1}[N]$-norm*, preprint `arXiv:2402.17994` (2024).

[9] J. Merikoski, *On Gaussian primes in sparse sets,* Compos. Math. **161** (2025), no. 2, 181–243.

Summary of the problem session

(Compiled by Thomas F. Bloom)

The following problems were discussed on the third evening of the workshop.

(Proposed by Edgar Assing)

Let $S_k(N)$ be the space of cusp forms of level N and weight k, equipped with the Petersson norm

$$\|f\|^2 = \int_{\Gamma_0(N)\backslash\mathbb{H}} |f(x+iy)|^2 y^{k-2} \mathrm{d}x\mathrm{d}y.$$

Any $f \in S_k(N)$ has a Fourier expansion of the form

$$f(z) = \sum_{n=1}^{\infty} a_f(n) n^{\frac{k-1}{2}} e(nz).$$

Is it true that, for every $\epsilon > 0$ there exists $C > 0$ depending only on k and ϵ such that

$$\|f\|^2 \ll_{k,\epsilon} \sum_{n \leq C \cdot N^{1+\epsilon}} |a_f(n)|^2 \quad \text{for all} \quad f \in S_k(N)? \tag{1}$$

Note that, since $\dim S_k(N) \asymp_k N^{1+o(1)}$, the length of the sum is essentially as short as possible. We can prove (1) in the special case when N is square-free and $f \in S_k(N)$ is an eigenfunction of all Atkin-Lehner operators. In [1] (1) is proved for all $f \in S_k(N)$, but with $N^{1+\epsilon}$ replaced by $N^{2+\epsilon}$.

(Proposed by Christian Bernert and Nuno Arala Santos)

Let $n \geq 1$ and $A \subset \{-n, \dots, n\} \backslash \{0\}$ be a set of size n such that, for every $1 \leq k \leq n$, either k or $-k$ is a member of A. Is it true that

$$|(A-A) \cap [1,n]| = (1-o(1))n?$$

Is it true that for any $B \subseteq \{1, \dots, n\}$ with $|B| \geq \epsilon n$

$$\sum_{a,b \in A} 1_B(a-b) \gg_\epsilon n^2?$$

Note that if we ask instead that either k or $1-k$ is a member of A then the answer is trivially no, since we could take A to contain only even integers. With k and $-k$ there do not seem to be any congruence obstructions.

(Proposed by Thomas F. Bloom)

(1) A problem of Erdős [4] (also recorded by Erdős in the Oberwolfach Problem Book in 1986). Recall that a positive integer n is 3-full if $p \mid n$ implies $p^3 \mid n$ for all primes p. Let A be the set of numbers which are the sum of three 3-full numbers.

(a) Does A have positive density? (Presumably yes, since the sums of three cubes should have positive density. Is this easier to prove for the sum of three 3-full numbers?)
(b) Are all sufficiently large integers in A? (Presumably not – indeed, probably the density of A is < 1. For the sums of three cubes this is either an easy counting argument or one can argue modulo 9, but both fail for the sums of three 3-full numbers.)

(2) A problem of Erdős and Ingham [5]. Let

$$f(s) = 1 + 2^{-s} + 3^{-s} + 5^{-s}.$$

Are there any $t \in \mathbb{R}$ such that $f(1 + it) = 0$? (Presumably not.) This was asked by Erdős and Ingham in connection with Tauberian theorems.

(Proposed by Julia Brandes)

(1) How many palindromic squares are there? There are infinitely many, but how many are there in $[1, X]$? *Editor's note: Keith* [9] *has given four infinite families of palindromic squares, and asks whether there are infinitely many aside from these.*
(2) How many non-palindromic squares are there which remain a square when the digits are reversed? For example 144 and 169. This is OEIS A033294. Are there infinitely many?

(Proposed by Tim Browning)

Let $N(B)$ count the number of solutions to

$$x^3 + 2xyz + xw^2 - y^2w + wz^2 = 0$$

with $x \neq 0$ and $\gcd(x, y, z, w) = 1$ with $x, y, z, w \in \mathbb{Z}^4 \cap [-B, B]^4$. This has 4 singularities, and is a twisted form of the Cayley cubic surface. Prove an asymptotic for $N(B)$ of the shape

$$N(B) \sim (c_1 + c_2)B(\log B)^3$$

with explicit constants $c_1, c_2 > 0$. The first constant c_1 is a product of local densities (with a value predicted by Peyre), but the other constant is more mysterious, coming from a Zariski dense thin set of rational points.

(Proposed by Jörg Brüdern)

Olson's theorem says that any set of $2p$ points in $\mathbb{F}_p^2$ contains a subset whose sum is zero. Lotter proved that this is true for any set of $p + 1$ points in $\mathbb{F}_p^2$, under the additional assumption that A contains one point on each line through the origin.

What is the proper generalisation of this to higher dimensions? In other words, find a natural geometric condition (perhaps formulated in terms of linear algebra) that ensures that any set of $p+n-1$ points in $\mathbb{F}_p^n$ satisfying this condition contains a subset whose sum is zero.

(Proposed by Brian Conrey)

Find a primitive degree 3 L-function which (provably) has infinitely many zeros on the critical line. (Or even just prove that at least one such L-function exists of degree ≥ 3.)

(Proposed by Dimitris Koukoulopoulos)

(1) Let $k \geq 7$ and $N_1 \leq \cdots \leq N_k$. Find the correct order of magnitude for

$$A_k(N_1, \ldots, N_k) = \#\{n_1 \cdots n_k : 1 \leq n_i \leq N_i\}.$$

When all $N_i = N$ this is the classic multiplication table problem, for which the exact order of magnitude was given by Ford [6] when $k = 2$ and Koukoulopoulos [10] when $k \geq 3$, namely

$$A_k(N) \asymp_k \frac{N^k}{(\log N)^{Q(\frac{k-1}{\log k})}(\log\log N)^{3/2}}$$

with $Q(x) = x \log x - x + 1$. This was generalised to the asymmetric problem for $2 \leq k \leq 6$ by Koukoulopoulos [11].

(2) Let $A \subset \mathbb{R}_{>1}$ be a countable set such that $\sum_{\alpha \in A} \frac{1}{\alpha \log \alpha}$ diverges. Prove that, for every $\epsilon > 0$, there exist distinct $\alpha, \beta \in A$ and an integer $n \geq 1$ such that $|\alpha - n\beta| < \epsilon$.

This is an old problem of Erdős, first asked in [3]. Koukoulopoulos, Lamzouri, and Lichtman [12] have recently proved this under the stronger condition that $\sum_{\alpha \in A \cap [1,x]} \frac{1}{\alpha} = o(\log x)$.

(Proposed by Emmanuel Kowalski)

Let

$$E : y^2 = x^3 + ax + b$$

be an elliptic curve defined over $\mathbb{Q}$. If $E(p)$ is the set of solutions modulo p then $|E(p)| = p + 1 - a_p$ for some $|a_p| \leq 2\sqrt{p}$, by Hasse's theorem. One can show by an elementary computation that if p does not divide the discriminant (or the conductor) of E, and if a_p is non-zero, then the multiplicative order of a_p modulo p coincides with the degree of the extension of $\mathbb{F}_p$ generated by the p-torsion points of E over $\mathbb{F}_p$.

(1) Are there infinitely many p such that a_p is a primitive root modulo p?
(2) Are there infinitely many p such that the order of a_p modulo p is ≥ 6? In the meeting Jori Merikoski sketched a solution for this.

(Proposed by Jori Merikoski)

Let $d(n)$ be the divisor function.

(1) Prove an asymptotic formula for

$$\sum_{m,n\le X} d(m^3+n^3+1).$$

Grimmelt and Merikoski [8] have given such an asymptotic for the sum of $d(mn^2+1)$.

(2) Prove that, for some suitable main term $f(X)$,

$$\sum_{p,q\le X} d(p^2+q^2) = f(X)(1+O((\log X)^{-10})).$$

(3) Prove that

$$\sum_{n\le X} d(n) \sum_{\substack{0\le a<n\\ a^2\equiv -1 \pmod n}} e\left(\frac{ha}{n}\right) \ll X^{1-\delta}$$

for some $\delta > 0$.

(Proposed by Mayank Pandey)

Let $F : [0,1]^2 \to \mathbb{R}$ be a smooth non-constant function and q be a large integer. Prove that, for any fixed $k \ge 1$ and $\delta > 0$, if $T \le q^k$ and

$$\left| \sum_{\substack{1\le a,b<q\\ (ab,q)=1}} e\left(TF\left(\tfrac{a}{q},\tfrac{b}{q}\right)\right)\right| < q^{2-\delta},$$

then there exists some $\delta' > 0$ (dependent only on k and δ) such that

$$\sum_{\substack{1\le a<q\\ (a,q)=1}} e\left(TF\left(\tfrac{a}{q},\tfrac{\overline{a}}{q}\right)\right) \ll_F q^{1-\delta'},$$

where $\overline{a}$ denotes the inverse of a modulo q.

(Proposed by Cedric Pilatte)

Let $A \subset \mathbb{N}$ be an infinite set and $S \subseteq [0,1]$ be a set of positive measure. If there exists a constant $C > 0$ such that

$$\left| \sum_{n\in A\cap[1,x]} e(n\alpha)\right| \le C$$

for every x and every $\alpha \in S$ then must A be eventually periodic? This was proved by Fregoli [7] if S contains an interval.

(Proposed by Trevor Wooley)

(1) Let $\alpha, \beta \in \mathbb{R}$ and

$$B = B(\alpha, \beta) = \{\lfloor \alpha m + \beta \rfloor : m \in \mathbb{N}\}.$$

Prove that

$$\int_0^1 \left| \sum_{n \in B \cap [1,N]} e(n\theta) \right|^p \mathrm{d}\theta \ll_{\alpha,\beta,p} \begin{cases} \log N & \text{when } p = 1, \text{ and} \\ N^{p-1} & \text{when } p > 1. \end{cases}$$

We can prove an upper bound of $\ll (\log N)^2$ when $p = 1$ and N^{p-1} for $p > 1$ provided α is of finite Diophantine type - that is, there exists some k such that

$$\liminf q^k \|q\alpha\| > 0.$$

(2) Say that a sequence (s_n) of real numbers is well-distributed modulo 1 if, for all $0 \leq a < b < 1$,

$$\lim_{N \to \infty} \sup_{m \geq 1} |N^{-1} \#\{n \leq N : \{s_{n+m}\} \in [a, b]\} - (b - a)| = 0.$$

Prove that, if p_n is the sequence of primes, the sequence αp_n is not well-distributed whenever α is irrational. Champagne, Le, Liu, and Wooley [2] have proved this for some specific constructed Liouville-type α, and also some α of finite Diophantine type.

References

[1] E. Assing, Y. Li, T. Wang, J. Xia, *Isogenies of CM Elliptic Curves*, arXiv:2503.05685 (2025).

[2] J. Champagne, T. Le, Y.-R. Liu, and T. D. Wooley, *Well-distribution modulo one and the primes*, preprint arXiv:2406.19491 (2024).

[3] P. Erdős, *Some unsolved problems*, Magyar Tud. Akad. Mat. Kutató Int. Közl. (1961), 221-254.

[4] P. Erdős, *Problems and results on number theoretic properties of consecutive integers and related questions*, Proceedings of the Fifth Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1975) (1976), 25-44.

[5] P. Erdős and A. E. Ingham, *Arithmetical Tauberian theorems*, Acta Arith. (1964), 341-356.

[6] K. Ford, *The distribution of integers with a divisor in a given interval*, Annals of Math. (2) 168 (2008), 367-433.

[7] R. Fregoli, *A note on bounded exponential sums*, Bull. Lond. Math. Soc. 53 (2021), 416–425.

[8] L. Grimmelt and J. Merikoski, *The divisor function along arithmetic progressions and binary cubic polynomials*, preprint arXiv:2508.17979 (2025).

[9] M. Keith, *Classification and enumeration of palindromic squares*, J. Rec. Math., 22 (No. 2, 1990), 124-132.

[10] D. Koukoulopoulos, *Localized factorizations of integers*, Proc. Lond. Math. Soc. (3) 101 (2010), no. 2, 392-426.

[11] D. Koukoulopoulos, *On the number of integers in a generalized multiplication table*, J. Reine Angew. Math. 689 (2014), 33-99.

[12] D. Koukoulopoulos, Y. Lamzouri and J. D. Lichtman, *Erdős's integer dilation approximation problem and GCD graphs*, preprint arXiv:2502.09539 (2025).

Reporter: Alexandru Pascadi

Participants

Nuno Miguel Arala Santos
Institut für Algebra, Zahlentheorie
und Diskrete Mathematik
Leibniz Universität Hannover
Welfengarten 1
30167 Hannover
GERMANY

Dr. Edgar Assing
Mathematisches Institut
Universität Bonn
Endenicher Allee 60
53115 Bonn
GERMANY

Dr. Benjamin Bedert
Centre for Mathematical Sciences
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

Dr. Christian Bernert
Institute for Science and Technology
Austria
Am Campus 1
3400 Klosterneuburg
AUSTRIA

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
School of Mathematics
The University of Manchester
Oxford Road
Manchester M13 9PL
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

Stephanie Chan
University College London
Department of Mathematics
Gower Street
London, WC1E 6BT
UNITED KINGDOM

Dr. Felicien Comtat
Mathematisches Institut
Universität Bonn
Endenicher Allee 60
53115 Bonn 53115
GERMANY

Prof. Dr. Brian Conrey
American Institute of Mathematics
California Institute of Technology
1200 E California Blvd.
Pasadena CA 91125
UNITED STATES

Prof. Dr. Cécile Dartyge
Institut Elie Cartan de Lorraine
et Institut Universitaire de France
Université de Lorraine
Faculté des Sciences et Technologies
Campus, Boulevard des Aiguillettes
54506 Vandœuvre-lès-Nancy
FRANCE

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

Prof. Dr. Alexander Dunn
School of Mathematics
Georgia Institute of Technology
686 Cherry Street
Atlanta, GA 30332-0160
UNITED STATES

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

Prof. Dr. Kevin Ford
Dept. of Mathematics, University of
Illinois at Urbana-Champaign
Urbana, IL 61801-2975
UNITED STATES

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

Dr. Oleksiy Klurman
Department of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW
UNITED KINGDOM

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

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

Dr. Vivian Kuperberg
Forschungsinstitut für Mathematik
ETH Zürich
8092 Zürich
SWITZERLAND

Dr. Junxian Li
Department of Mathematics
University of California, Davis
One Shields Avenue
Davis CA 95616-8633
UNITED STATES

Dr. Vlad Matei
Institute of Mathematics
"Simion Stoilow"
of the Romanian Academy
P.O. Box 1-764
014 700 Bucharest
ROMANIA

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

Prof. Dr. Lilian Matthiesen
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstraße 3-5
37073 Göttingen
GERMANY

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

Dr. Jori Merikoski
Mathematical Institute
University of Oxford
Andrew Wiles Building
Radcliffe Observatory Quarter
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Mayank Pandey
Department of Mathematics
Princeton University
Fine Hall
Washington Road
Princeton CA 08544-1000
UNITED STATES

Dr. Alexandru Pascadi
Mathematisches Institut
Universität Bonn
Endenicher Allee 60
53115 Bonn
GERMANY

Dr. Sarah Peluse
Department of Mathematics
Stanford University
Stanford, CA 94305-2125
UNITED STATES

Dr. Dan Petersen
Department of Mathematics
Stockholm University
106 91 Stockholm
SWEDEN

Cédric Pilatte
Mathematical Institute
Oxford University
Andrew Wiles Building
Woodstock Rd
Oxford OX2 6GG
UNITED KINGDOM

Dr. Sean Prendiville
School of Mathematical Sciences
Lancaster University
Lancaster LA1 4YX
UNITED KINGDOM

Prof. Dr. Maksym Radziwiłł
Department of Mathematics
Northwestern University
2033 Sheridan Road
Evanston IL 60208-2730
UNITED STATES

Dr. Simon L. Rydin Myerson
Department of Mathematical Sciences
Chalmers University of Technology and
University of Gothenburg
412 96 Göteborg
SWEDEN

Prof. Dr. Mehtaab Sawhney
Department of Mathematics
Columbia University
Mathematics Hall, 2990 Broadway
New York City, NY 10027
UNITED STATES

Leo Schäfer
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstraße 3-5
37073 Göttingen
GERMANY

Prof. Dr. Damaris Schindler
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstr. 3-5
37073 Göttingen
GERMANY

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

Julia Stadlmann
Department of Mathematics
University of Illinois at
Urbana-Champaign
Harker Hall
Urbana IL 61801
UNITED STATES

Dr. Niclas Technau
Department of Mathematics
University of Wisconsin-Madison
480 Lincoln Drive
Madison, WI 53706-1388
UNITED STATES

Dr. Joni Teräväinen
Department of Pure Mathematics and
Mathematical Statistics,
University of Cambridge
Cambridge CB3 0WB
UNITED KINGDOM

Prof. Dr. Robert C. Vaughan
335 McAllister Building
Department of Mathematics
Pennsylvania State University
Pollock Road
State College, PA 16802
UNITED STATES

Mieke Wessel
École Polytechnique/INRIA Saclay
1 Rue Honoré d'Etienne D'Orves
91120 Palaiseau Cedex
FRANCE

Katharine Woo
Department of Mathematics
Stanford University
Stanford CA 94305-2125
UNITED STATES

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

Dr. Nina Zubrilina
Department of Mathematics
Massachusetts Institute of
Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES