Mathematisches Forschungsinstitut Oberwolfach

Report No. 52/2025

DOI: 10.4171/OWR/2025/52

Arithmetic Statistics for Algebraic Objects

Organized by
Lior Bary-Soroker, Tel Aviv
Alina Ostafe, Sydney
Peter Sarnak, Princeton

9 November – 14 November 2025

Abstract. The workshop focused on various directions of *arithmetic statistics* in algebra and number theory. These include statistical problems for random polynomials and varieties, probabilistic Galois theory, and counting and distribution problems for algebraic functions, algebraic number fields, elliptic curves, L-functions, as well as arithmetic problems in non-abelian settings (eg, arithmetic statistics for algebraic groups).

Mathematics Subject Classification (2020): Primary: 11-XX; Secondary: 12-XX, 14Gxx.

Introduction by the Organizers

Arithmetic Statistics is a branch of Number Theory concerned with counting and distribution problems for such fundamental objects as polynomials, algebraic number fields, elliptic curves, L-functions, modular forms, integral matrices, etc, where much progress has been made in the last decades. The aim of the workshop was to focus on recent breakthroughs on statistical aspects of algebraic objects, which have not received as much attention in recent workshops as they deserve. These include random polynomials and varieties, multiplicative arithmetic functions, specialisation problems for algebraic functions and connections to other areas (such as arithmetic geometry), and various statistics for arithmetic groups (e.g., arithmetic statistics of integer matrices satisfying certain properties). The topic for this workshop has seen many breakthroughs towards longstanding problems and conjectures (van der Wearden conjecture, function field versions of the Twin Prime conjecture and its generalisations, the Schinzel Hypothesis H and the Bateman-Horn conjecture, the Hasse principle, the Hilbert Irreducibility Theorem, statistics of arithmetic groups, to mention just a few). One key aspect in these developments is the vast arsenal of tools from different areas that had to be developed.

The workshop brought together distinguished experts and younger researchers (46 attending in person and one online) from 12 countries (with 8 from Germany) with backgrounds ranging from algebraic and analytic number theory, to random matrix theory, group theory and arithmetic geometry. We had 28 excellent talks, each of 30 min length, with an open problem session on Monday evening. We also allowed plenty of time for participants to have informal discussions and work on problems of interest.

More precisely, the talks focused on the following main directions:

- Distribution properties of L-functions: *talks by V. Blomer, S. Drappeau, M. Lalin, I. Shparlinski.* The talks included reports on recent advances on central values of L-functions and their twists generating the number field generated by its Dirichlet coefficients, results on moments, vanishing and large values of L-functions in thin families and over function fields.
- Random polynomials and probabilistic Galois theory: *talks by D. Hokken, A. Entin, R. Dietmann, V. Matei, M. Wenqiang Xu.* Advances in this direction include, but not limited to: a new upper bound for the number of number fields of bounded discriminant and prescribed even Galois group, new results on the irreducibility of several models of polynomials with restricted coefficients, as well as the state of art in the study of Galois groups of random polynomials over function fields.
- Distribution of other algebraic objects (including number fields, function fields, elliptic curves, Selmer groups): *talks by M. Matchett Wood, D. Neftin, S. W. Park, M. Shusterman, A. Swaminathan.* We especially highlight the work of Matchett Wood and Sawin which introduces a new moment method for algebraic objects that allows one to determine a distribution from its expected number of surjections onto each finite object. Three applications were discussed, to fundamental groups of 3-manifolds, the class groups of extensions of number fields with roots of unity, and to distributions of fundamental groups of curves over finite fields.
- Distribution of rational points on varieties: *talks by A. Fehm, E. Sofos, C. Stewart, N. Technau, E. Viada, K. Woo.* Reported advances include, but not limited to: a result showing that the Hasse principle holds for 100% of conic bundles, sharp estimates for the number of rational points of bounded (naive) height near non-degenerate curves in $\mathbb{R}^3$, and various counting results for integral or rational points on varieties.
- Character sums and automorphic forms: *talks by E. Fouvry, N. Kimmel, P. Michel, M. Pandey.* Results included new bounds on certain character sums over polynomial values, on bilinear sums of traces functions well below the Pólya-Vinogradov range, as well as power-saving estimates for sums of (GL(3) and GL(2)) divisor function and automorphic form coefficients along binary cubic and quartic forms.

- Arithmetic statistics in noncommutative settings: *talks by D. Garzoni, T. Browning, B. Rodgers, V. Wang.* Advances include developing a circle method in the non-commutative setting and its applications to counting problems, as well as obtaining new results on the arithmetic statistics of commuting matrices.

The extended abstracts below will give a detailed account of the main results reported during the workshop. Furthermore to the aforementioned talks, the participants had many productive discussions and worked in small groups on joint projects (new and old) during the workshop, thus we expect that the outcomes of these collaborations will have a significant impact on the area long after the workshop. In fact, two participants, O. Klurman and V. Matei, already submitted a preprint on arxiv (https://arxiv.org/abs/2511.10359) based on their work during the workshop.

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: Arithmetic Statistics for Algebraic Objects

Table of Contents

Abstracts

Hecke fields: Galois theory meets shifted convolution sums

Valentin Blomer
(joint work with A. Burungale, P. Michel and J.-H. Min)

Let $f(z) = \sum_n a_n e(nz)$ be a holomorphic Hecke cusp form and χ a primitive Dirichlet character. Associated to these two objects are the algebraic number fields $\mathbb{Q}(f) = \mathbb{Q}(\{a_n \mid n \in \mathbb{N}\})$ and $\mathbb{Q}(\chi) = \mathbb{Q}(\{\chi(n) \mid n \in \mathbb{N}\})$ as well as their composite $\mathbb{Q}(f, \chi)$. Shimura [5] showed the following remarkable algebraicity result: there exists $\Omega_{f,\pm} \in \mathbb{C}^*$ such that

$$L_f(\chi) := \frac{G(\bar{\chi})L(1/2, f \times \chi)}{\Omega_{f,\mathrm{sgn}(\chi)}} \in \mathbb{Q}(f, \chi)$$

(where G denotes a normalized Gauß sum) along with the reciprocity law $\sigma L_f(\chi) = L_{f^\sigma}(\chi^\sigma)$ for $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

For an odd prime p and $h \geq 2$ we consider the following set of "wild" Dirichlet characters

$$\Xi_{p,h} := \{\chi \mid \mathrm{cond}(\chi) = p^h, \mathrm{ord}(\chi) = p^{h-1}\},$$

which forms a Galois orbit. We think of f and p as fixed and vary h. Important results of Luo–Ramakrishnan [4] and Sun [6] state almost all values $L^{\mathrm{alg}}(f \times \chi)$ (essentially) generate $\mathbb{Q}(f, \chi)$. More precisely: for all $h \geq h_0$ and all $\chi \in \Xi_{p,h}$ we have $\mathbb{Q}(f, \chi) = \mathbb{Q}(\mu_p, L_f(\chi))$ where μ_p denotes the p-th roots of unity. Here we prove an analogous result for squares [1]:

Theorem 1. *Suppose that f is a non-CM form with no non-trivial quadratic inner twists, and let $p \geq p_0(f)$ be a prime. Then for all but finitely many $\chi \in \Xi_{p,h}$ we have*

$$\mathbb{Q}(f, \chi) = \mathbb{Q}(\mu_p, |L_f(\chi)|^2).$$

To show Theorem 1, we need to show the two inclusions

$$\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\mu_p, |L_f(\chi)|^2), \quad \mathbb{Q}(f) \subseteq \mathbb{Q}(\chi, |L_f(\chi)|^2).$$

An inspection of the field diagram

$$\begin{tikzcd}
 & \mathbb{Q}(f,\chi) \arrow[d, dash] \arrow[ddrr, dash, dotted] & & & & \\
 & \mathbb{Q}(\chi, |L_f(\chi)|^2) \arrow[dl, dash] \arrow[dr, dash] & & & E(\chi) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\chi) \arrow[dr, dash] & & \mathbb{Q}(\mu_p, |L_f(\chi)|^2) \arrow[dl, dash] & E \arrow[d, dash] \arrow[dr, dash] & & \mathbb{Q}(\chi, |L_f(\chi)|^2) \arrow[dl, dash] \\
 & \mathbb{Q}(\chi) \cap \mathbb{Q}(\mu_p, |L_f(\chi)|^2) \arrow[d, dash] & & \mathbb{Q}_f & E \cap \mathbb{Q}(\chi, |L_f(\chi)|^2) & \\
 & \mathbb{Q} \arrow[urr, dash, dotted] & & & &
\end{tikzcd}$$

(where E is the Galois closure of $\mathbb{Q}(f)$) shows that these two inclusions follow if we can evaluate asymptotically expressions of the type

$$\sum_{\chi \in \Xi_{p,h}} |L(1/2, f \times \chi)|^2 \chi(r) \tag{1}$$

and small generalizations thereof for fixed $r \in \mathbb{N}$. This translates the problem of finding a generator of $\mathbb{Q}(f,\chi)$ into a problem of mean values of L-functions. By an approximate functional equation and some approximate orthogonality in the set $\Xi_{p,h}$, we arrive at a shifted convolution sums roughly of the shape

$$\sum_{\substack{\alpha m \equiv rn \,(\mathrm{mod}\ q) \\ mn \leq q^2}} \lambda_f(m)\lambda_f(n) \tag{2}$$

where $q = p^h$, α is a $(p-1)$-st root of unity modulo q and λ_f are the normalized Hecke eigenvalues of f.

If $\alpha = 1$, this is a familar expression that has been analyzed for instance in [3], using a combination of spectral theory of automorphic forms and bounds for linear forms in Kloosterman sums for suitably factorizable moduli.

When $\alpha \neq 1$, then every representative of α is automatically of power growth in q (namely at least of size $q^{1/(p-1)}$), which is not compatible with the spectral methods in [3]. For such α, we use a completely different technique inspired by [2], which provides a resolution of unipotent mixing conjecture. We sacrifice any cancellation in the expression and apply absolute values to each summand. This allows us to use sieving techniques for multiplicative functions, exploiting the facts that (a) by Sato–Tate the Hecke eigenvalues are a little less than one on average over primes, and (b) the two-dimensional lattice defined by $\alpha m \equiv rn \,(\mathrm{mod}\ q)$ is somewhat round (i.e. its minimum is $\gg q^{1/(p-1)}$). This allows us to bound (2) with a saving of a small power of $\log q$ relative to the main term of (1).

References

[1] V. Blomer, A. Burungale, P. Michel. J.-H. Min, Generation of Hecke fields by squares of cyclotomic twists of modular L-values, `arXiv:2503.15040`

[2] V. Blomer, P. Michel. The unipotent mixing conjecture. Journal d'Analyse Math. 151 (2023), 25–57

[3] V. Blomer, D. Milćević. The second moment of twisted modular L-functions. Geometric and Functional Analysis 25 (2015), 453–516

[4] W. Luo, D. Ramakrishnan. Determination of modular forms by twists of critical L-values. Invent. math. 130 (1997), 371–398

[5] G. Shimura. On the periods of modular forms. Math. Ann. 229 (1977), 211–221

[6] H.-S. Sun. Generation of cyclotomic Hecke fields by modular L-values with cyclotomic twists. Amer. J. Math. 141 (2019), 907–940

Nonvanishing of L–functions associated to fixed order characters over function fields

Matilde Lalin

(joint work with Chantal David, Alexandra Florea)

We consider the family of Dirichlet L–functions over the rational function field $\mathbb{F}_q(T)$ (where q is a prime power) attached to characters of *fixed order* $\ell \geq 3$. Let $\mathcal{H}_d$ denote the set of monic squarefree polynomials of degree d on $\mathbb{F}_q[T]$. We prove that a *positive proportion* of the central values $L(\frac{1}{2}, \chi_c)$ in the thin family

$$\mathcal{F}_\ell(d) \;=\; \left\{\chi_c = \left(\frac{c}{\cdot}\right)_\ell, c \in \mathcal{H}_d\right\},$$

where $\left(\frac{c}{\cdot}\right)_\ell$ denotes the ℓ-power symbol modulo c, are nonzero as $d \to \infty$.

Nonvanishing in families of Dirichlet L-functions over the integers has a long history (Iwaniec–Sarnak [IS99], Soundararajan [Sou00], Baier–Young [BY10], among others). In the function field setting, positive proportion results were known for quadratic and cubic families (Bui–Florea [BF18], David–Florea–Lalín [DFL21]), and positive results with zero density were also obtained in thin subfamilies for larger ℓ (Ellenberg–Li–Shusterman [ELS20]).

For $\chi_c \in \mathcal{F}_\ell(d)$ an (odd) Dirichlet character over $\mathbb{F}_q(T)$, the L–function

$$\mathcal{L}(u, \chi_c) \;=\; \prod_{j=1}^{d-1} \left(1 - q^{1/2} e^{-2\pi i \theta_{c,j}} u\right)$$

is a polynomial whose inverse zeros lie on the circle $|u| = q^{1/2}$ by the Riemann Hypothesis over function fields.

Let ϕ be an even test function in the Schwartz space whose Fourier transform $\widehat{\phi}$ is compactly supported. We consider

$$\Phi(\theta) := \sum_{k\in\mathbb{Z}} \phi((d-1)(\theta - k)) \text{ and } \Sigma(\phi, \chi_c) := \sum_{j=1}^{d-1} \Phi\left(\theta_{c,j}\right).$$

The one-level density of zeros is defined to be the limit as $d \to \infty$ of the average

$$\langle \Sigma(\phi, \chi_c) \rangle_{\mathcal{F}_\ell(d)} := \frac{1}{|\mathcal{F}_\ell(d)|} \sum_{\chi_c \in \mathcal{F}_\ell(d)} \Sigma(\phi, \chi_c).$$

Theorem 1. [DFL25, Theorem 1.1] *Let ℓ and q such that $q \equiv 1 \pmod{2\ell}$. Let $d \not\equiv 0 \pmod{\ell}$. Let ϕ be an even test function in the Schwartz space $\mathcal{S}(\mathbb{R})$ whose Fourier transform is supported in $(-v, v)$ such that*

$$v \leq \begin{cases} \frac{6}{5}, & \ell = 3, \\ \frac{26}{23}, & \ell = 4, \\ \frac{2\ell^2+\ell-2}{2\ell^2-\ell+2}, & 5 \leq \ell \leq 8, \\ \frac{3\ell^2-7\ell-2}{3\ell^2-9\ell+2}, & \ell = 9, 10, \\ \frac{9\ell^2-25\ell-6}{9\ell^2-31\ell+6}, & 11 \leq \ell. \end{cases}$$

Then

$$\langle \Sigma(\phi, \chi_c) \rangle_{\mathcal{F}_\ell(d)} = \widehat{\phi}(0) + O\left(\frac{1}{d}\right).$$

If $\widehat{\phi}$ is supported in $(-v, v)$, then the one-level density controls the proportion of central zeros, yielding a nonvanishing proportion of $1 - \frac{1}{v}$.

Corollary 2. [DFL25, Corollary 1.2] *Let $q \equiv 1 \pmod{2\ell}$ and $\ell \nmid d$. Then for $d \to \infty$,*

$$\frac{\#\{\chi_c \in \mathcal{F}_\ell(d) : \ L(\frac{1}{2}, \chi_c) \neq 0\}}{\#\mathcal{F}_\ell(d)} \geq \begin{cases} \frac{1}{6}, & \ell = 3, \\ \frac{3}{26}, & \ell = 4, \\ \frac{2(\ell-2)}{2\ell^2+\ell-2}, & 5 \leq \ell \leq 8, \\ \frac{2(\ell-2)}{3\ell^2-7\ell-2}, & \ell = 9, 10, \\ \frac{6(\ell-2)}{9\ell^2-25\ell-6}, & 11 \leq \ell. \end{cases}$$

Ideas in the proof We start by applying the Explicit Formula, which relates sums of zeros of L-functions to sums of powers of monic irreducible polynomials.

$$\langle \Sigma(\phi, \chi_c) \rangle_{\mathcal{F}_\ell(d)} = \widehat{\phi}(0) - \frac{1}{d|\mathcal{H}_d|} \sum_{1 \leq n \leq vd} \widehat{\phi}\left(\frac{n}{d}\right) \sum_{c \in \mathcal{H}_d} \sum_{f \in \mathcal{M}_n} \frac{\Lambda(f)(\chi_c(f) + \overline{\chi_c(f)})}{|f|^{\frac{1}{2}}}.$$

The contribution of prime powers is negligible. After removing the square-free condition on c, we apply Poisson summation, which shortens the sum but introduces ℓ-order Gauss sums

$$G_\ell(V, R) := \sum_{a \pmod{R}} \left(\frac{a}{R}\right)_\ell e_q\left(\frac{Va}{R}\right).$$

More precisely, we obtain

$$\sum_{P \in \mathcal{P}_n} \frac{\deg(P)}{|P|^{\frac{1}{2}}} \sum_{c \in \mathcal{M}_d} \chi_c(P) \rightsquigarrow \sum_{V \in \mathcal{M}_{n-d}} \sum_{\substack{P \in \mathcal{P}_n \\ (P,V)=1}} G_\ell(V, P).$$

Since ℓ-order Gauss sums are not multiplicative, standard methods for quadratic Gauss sums do not apply. Following Heath-Brown [HB95, HB00], we use Vaughan's identity to rewrite the sum as a combination of Type I and Type II terms. The Type II sums, of large length, are bounded independently of ℓ via Cauchy–Schwarz and the Large Sieve of Blomer–Goldmakher–Louvel [BGL14]. The Type I sums, of short length, lead to expressions of the form

$$\sum_{V\in\mathcal{M}_{n-d}} \sum_{\substack{b\in\mathcal{H} \\ \deg(b)\le U}} \sum_{\substack{c\in\mathcal{M}_n \\ b|c \\ (c,V)=1}} G_\ell(V,c).$$

After some combinatorial reductions, we are led to study the generating series

$$\psi_\ell^{(i)}(V;u) = (1-q^\ell u^\ell)^{-1} \sum_{\substack{F\in\mathcal{M} \\ \deg(F)\equiv i \pmod{\ell}}} G_\ell(V,F)u^{\deg(F)},$$

which, by Hoffstein [Hof92] and Patterson [Pat07], is a rational function satisfying a functional equation and having poles at $u^\ell = q^{-\ell-1}$. To obtain our bounds, we estimate $\psi_\ell^{(i)}(V;u)$ near its poles using convexity bounds, the Phragmén–Lindelöf principle for smaller ℓ, and Lindelöf-on-average estimates deduced from applying the Large Sieve again after using an approximate functional equation that shortens the numerator of the rational expression of $\psi_\ell^{(i)}(V;u)$.

Cancellation of Gauss sums along primes We also obtain an average of ℓ-order Gauss Sums twisted by $V\in\mathbb{F}_q[T]$ and indexed by primes $P\in\mathbb{F}_q[T]$ of fixed degree n with $(P,V)=1$. We show strong cancellations in the prime average:

$$\sum_{P\in\mathcal{P}_n} G_\ell(V,P) \ \ll\ q^{n\cdot\alpha(\ell)+\varepsilon n}\,|V|^{\beta(\ell)+\varepsilon},$$

with explicit exponents $\alpha(\ell),\beta(\ell)$ that sharpen classical square-root bounds. For instance, when $\ell>8$ one can take

$$\alpha(\ell) = \tfrac{3}{2} - \tfrac{\ell-2}{\ell^2}, \qquad \beta(\ell) = \tfrac{\ell^2-7\ell-2}{2\ell^2}.$$

These bounds are of independent interest (e.g. for equidistribution phenomena suggested by Weyl's criterion).

References

[BF18] H. M. Bui and Alexandra Florea, *Zeros of quadratic Dirichlet L-functions in the hyperelliptic ensemble*, Trans. Amer. Math. Soc. **370** (2018), no. 11, 8013–8045.

[BGL14] Valentin Blomer, Leo Goldmakher, and Benoît Louvel, *L-functions with n-th-order twists*, Int. Math. Res. Not. IMRN (2014), no. 7, 1925–1955.

[BY10] Stephan Baier and Matthew P. Young, *Mean values with cubic characters*, J. Number Theory **130** (2010), no. 4, 879–903.

[DFL21] Chantal David, Alexandra Florea, and Matilde Lalin, *Nonvanishing for cubic L-functions*, Forum Math. Sigma **9** (2021), Paper No. e69, 58.

[DFL25] Chantal David, Alexandra Florea, and Matilde Lalin, *Nonvanishing of L–functions associated to fixed order characters over function fields*, 2025.

[ELS20] Jordan S. Ellenberg, Wanlin Li, and Mark Shusterman, *Nonvanishing of hyperelliptic zeta functions over finite fields*, Algebra Number Theory **14** (2020), no. 7, 1895–1909.

[HB95] D. R. Heath-Brown, *A mean value estimate for real character sums*, Acta Arith. **72** (1995), no. 3, 235–275.

[HB00] ———, *Kummer's conjecture for cubic Gauss sums*, Israel J. Math. **120** (2000), no. part A, 97–124.

[Hof92] Jeffrey Hoffstein, *Theta functions on the n-fold metaplectic cover of* SL(2)*—the function field case*, Invent. Math. **107** (1992), no. 1, 61–86.

[IS99] H. Iwaniec and P. Sarnak, *Dirichlet L-functions at the central point*, Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, pp. 941–952.

[Pat07] S. J. Patterson, *Note on a paper of J. Hoffstein*, Glasg. Math. J. **49** (2007), no. 2, 243–255.

[Sou00] K. Soundararajan, *Nonvanishing of quadratic Dirichlet L-functions at* $s = \frac{1}{2}$, Ann. of Math. (2) **152** (2000), no. 2, 447–488.

The Galois group of random reciprocal polynomials

David Hokken

(joint work with Dimitris Koukoulopoulos)

The Galois group G_f of a polynomial $f \in \mathbb{Z}[x]$, say of degree n, captures the algebraic symmetries between the zeros of f. When f is squarefree, we can naturally view G_f as a permutation group contained in S_n, acting on the zeros $\alpha_1, \ldots, \alpha_n$. The only way in which $G_f \not\simeq S_n$ is when there is some, at times hardly visible, conspiracy between the α_j; in fact, the general philosophy (which has its origin already in the work of Hilbert [5]) is that such conspiracies are very unlikely to occur and thus that $G_f \simeq S_n$ for 'typical' f.

To make this more precise, consider the following setup. Given an integer $H \geq 2$ and random variables $a_0, a_1, \ldots$ taking values uniformly and independently in the set $[1, H] \cap \mathbb{Z}$, define the random monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$. Of course, there are many other natural ways to come up with a 'structured' family of random polynomials, so we have already severely restricted the scope here; in particular, most of the results discussed below hold in greater generality, where the set of allowed coefficients, the uniformity and independence assumptions can all be relaxed to some extent.

In the classical *large box model*, we fix $n \geq 1$ and let H tend to infinity. Van der Waerden [9] already gave an elementary proof that $G_f \simeq S_n$ with probability tending to 1; his lasting conjecture that $\mathbf{P}(G_f \not\simeq S_n) = \mathbf{P}(f \text{ is reducible}) + o(H^{-1})$ was — after many efforts — recently almost completely resolved by Bhargava [3]; it only remains to improve their bound $\mathbf{P}(G_f \simeq A_n) = O(H^{-1})$, with A_n denoting the alternating group, to $o(H^{-1})$.

In the *restricted coefficient model*, instead we fix H and let n tend to infinity. Odlyzko and Poonen [8] stated as a folklore conjecture that a random $0,1$-polynomial P of degree n is irreducible with high probability, conditioning on $P(0) \neq 0$. Konyagin [7] showed that such P has no factors of degree $\leq n/\log n$ with high probability. Conditional on the extended Riemann hypothesis, Breuillard and Varjú proved the Odlyzko–Poonen conjecture with an explicit description of the error term, moreover showing that $G_P \geq A_n$ with high probability. Shortly after, Bary-Soroker, Koukoulopoulos and Kozma gave an unconditional proof that

f, as in the model above with $H \geq 35$ fixed, has Galois group $G_f \geq A_n$ with probability $\geq 1 - n^{-c}$ for some absolute constant $c > 0$, for n large enough.

In joint work with Dimitris Koukoulopoulos [6], we study random monic *reciprocal* polynomials f of even degree $n = 2m$. These are the polynomials of the form

$$f(x) = x^{2m} + a_{m-1}x^{2m-1} + \cdots + a_0 x^m + \cdots + a_{m-1}x + 1.$$

Bhargava's result in the large box model has already been adapted to the setting of reciprocal polynomials by Anderson, Bertelli and O'Dorney [1]. We work in the restricted coefficient model, and prove that the irreducibility result of Bary-Soroker, Koukoulopoulos and Kozma continues to hold in this setting: that is, f is still irreducible with probability $\geq 1 - n^{-c}$ for some absolute constant $c > 0$ and n sufficiently large. Observe, however, that the Galois group of such reciprocal polynomials is much smaller than S_{2m}: the relation $f(x) = x^{2m} f(1/x)$ implies that the zeros of f come in pairs $\{\alpha_j, 1/\alpha_j\}$. For that reason, the maximal Galois group f could have is the *hyperoctahedral group* $C_2 \wr S_m$, which is an example of a permutational wreath product. Whereas A_n is the only 'large' proper subgroup of S_n (i.e., of bounded index in S_n as $n \to \infty$), the group $C_2 \wr S_m$ has four 'large' subgroups: the index 2 subgroups $C_2 \wr A_m$, $(C_2 \wr S_m) \cap A_{2m}$ and a harder to describe subgroup that we denote by G_2; intersecting these three groups yields the index 4 subgroup $(C_2 \wr A_m) \cap A_{2m}$. We show that G_f contains at least one of $C_2 \wr A_m$ and G_2 with high probability.

That we can obtain results so similar to those in [2], even though the family of reciprocal polynomials is so sparse in the set of all polynomials (think for comparison of the set of palindromic integers), is thanks to the extra structure that reciprocal polynomials admit. In particular, each reciprocal f of degree $2m$ has a unique *trace polynomial* $f_{\mathsf{R}} \in \mathbf{Z}[x]$ of degree m with the property that $f(x) = x^m f_{\mathsf{R}}(x + 1/x)$, and there is a correspondence between the divisors of f_{R} and the reciprocal divisors of f. A quick consequence is the following: if f is reducible, then it either has a reciprocal divisor of degree $\leq m$, or it has the 'special factorisation' $f(x) = g(x)x^m g(1/x)$ for some nonreciprocal $g \in \mathbf{Z}[x]$ of degree m. We treat the first possibility with the Fourier analytic methods of [2], although extra care is needed because of the dependencies between the coefficients of f. We rule out the special factorisation by means of random walk techniques, which also allow us to show that $G_f \not\leq A_{2m}$ with high probability. For the latter, it is extremely helpful that the reciprocity of f implies that its discriminant is a nonzero square if and only if f is separable and $(-1)^m f(1)f(-1)$ is a square.

References

[1] T. C. Anderson, A. Bertelli and E. M. O'Dorney, *Galois groups of reciprocal polynomials and the Van der Waerden–Bhargava theorem*, preprint arXiv:2406.18970, 21 pp.

[2] L. Bary-Soroker, D. Koukoulopoulos, and G. Kozma, *Irreducibility of random polynomials: general measures*, Invent. Math. **233** (2023), 1041–1120.

[3] M. Bhargava, *Galois groups of random integer polynomials and van der Waerden's conjecture*, Ann. of Math. (2) **201** (2025), 339–377.

[4] E. Breuillard and P. Varjú, *Irreducibility of random polynomials of large degree*, Acta Math. **223** (2019), 195–249.

[5] D. Hilbert, *Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. **110** (1892), 104–129.

[6] D. Hokken and D. Koukoulopoulos, *Irreducibility and Galois groups of random reciprocal polynomials of large degree*, preprint arXiv:2510.18857, 47 pp., 2025.

[7] S. V. Konyagin, *On the number of irreducible polynomials with* 0, 1 *coefficients*, Acta Arith. **88** (1999), 333–350.

[8] A. Odlyzko and B. Poonen, *Zeros of polynomials with* 0, 1 *coefficients*, Enseign. Math. (2) **39** (1993), 317–348.

[9] B. L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monatsh. Math. Phys. **43** (1936), 133–147.

Irreducibility of the characteristic polynomials of random tridiagonal matrices

Daniele Garzoni

(joint work with Lior Bary-Soroker and Sasha Sodin)

In recent years the study of random polynomials over the integers attracted much attention. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ where $a_0, \ldots, a_{n-1}$ are independent Rademacher random variables – that is, a_i takes value ± 1, each with probability $1/2$. A folklore conjecture predicts then $f(X)$ is irreducible in $\mathbf{Q}[X]$ with probability tending to one as $n \to \infty$. Recently, Breuillard–Varjú [6] proved the conjecture conditionally on the Extended Riemann Hypothesis. See Bary-Soroker–Kozma–Koukoulopoulos [2] for related strong unconditional results.

In fact, there is nothing special about the Rademacher distribution: A random polynomial of large degree should be irreducible with high probability, regardless of the specific chosen probability measure (and provided there is no obvious reason for which each polynomial in the given model must be reducible).

A natural way to construct a random polynomial is to look at the characteristic polynomial of a random matrix, which brings us into the world of discrete matrix theory. Let $A = (a_{i,j})$ be an $n \times n$ matrix whose entries $a_{i,j}$ are independent Rademacher random variables, and let $P_n(X)$ be the characteristic polynomial of A. Babai and Vu conjectured that $P_n(X)$ should be irreducible with probability tending to one as $n \to \infty$, and indeed, the probability should be of the form $1 - O(e^{-cn})$ for an absolute constant $c > 0$. To illustrate the breadth of the conjecture, let us note that it implies that A is nonsingular with probability $1 - O(e^{-cn})$, which is a breakthrough result of Kahn–Komlós–Szemerédi [11] and Tikhomirov [12] (the latter in a stronger form).

Eberhard [7] proved the conjecture conditionally on the Extended Riemann Hypothesis. Ferber–Jain–Sah–Sawhney [8] proved the same for random symmetric matrices, and once again, the same should be true for virtually any model of random matrices.

In joint work with Lior Bary-Soroker and Sasha Sodin [1], we address the case of random tridiagonal matrices. Namely, let $V_1, V_2, V_3, \cdots$ be independent

Rademacher and let $P_n(X)$ be the characteristic polynomial of

$$\begin{pmatrix} V_1 & 1 & 0 & 0 & 0 & \cdots \\ 1 & V_2 & 1 & 0 & 0 & \cdots \\ 0 & 1 & V_3 & 1 & 0 & \cdots \\ \vdots & & \ddots & \ddots & \ddots & \\ 0 & & \cdots & 1 & V_{n-1} & 1 \\ 0 & & \cdots & 0 & 1 & V_n \end{pmatrix}.$$

Conditionally on the Extended Riemann Hypothesis, we prove that $P_n(X)$ is irreducible with probability $1 - O(e^{-cn})$.

In addition to the irreducibility of random polynomials, part of the motivation and the method of proof is inspired from the world of continuous matrix theory and theoretical physics, and specifically from the theory of Schrödinger operators, see [3].

In the proof, we crucially use a method introduced by Breuillard–Varjú [6], which allows one to prove the irreducibility of a random polynomial $f(X)$ by studying the average number of roots of $f(X)$ modulo a large prime. This part of the proof, which is common to all the results from [6, 7, 8] mentioned above, is where the Extended Riemann Hypothesis is used. We are therefore reduced to a problem "modulo p", which is now a separate problem in each of the different models. In our case, we are naturally reduced to a problem of equidistribution of random walks in Cayley graphs of $\mathrm{SL}_2(\mathbf{F}_p)$, where we crucially use deep results of Bourgain–Gamburd–Sarnak [4], Breuillard–Gamburd [5] and Helfgott [10].

We also prove that the Galois group of $f(X)$ is A_n or S_n with probability $1 - O(e^{-cn})$. This is not a straightforward extension: We use the Classification of Finite Simple groups, as well as a result of Golsefidy–Srinivas [9] on expansion in direct products of $\mathrm{SL}_2(\mathbf{F}_p)$.

As for all results mentioned above, the V_i can be replaced by much more general random variables, and it is not really needed to have 1's above and below the diagonal. However, it should be pointed out that a key difference occurs if we assume that all the entries on the main diagonal are equal. To fix the ideas, let us assume that n is even, that the V_i are zero and that above and below the main diagonal we have Rademacher random variables. Then, it is not hard to see that the roots of $f(X)$ come in pairs $\alpha, -\alpha$. In particular, the Galois group of $f(X)$ is contained in a wreath product $C_2 \wr S_{n/2}$. We show that with probability $1 - O(e^{-cn})$ the Galois group contains the derived subgroup of $C_2 \wr S_{n/2}$ (which has index 4 therein).

References

[1] L. Bary-Soroker, D. Garzoni and S. Sodin, *Irreducibility of the characteristic polynomials of random tridiagonal matrices*, J. Number Theory **280** (2026), 973–998.

[2] L. Bary-Soroker, D. Koukoulopoulos and G. Kozma, *Irreducibility of random polynomials: general measures*, Invent. Math. **233** (2023), 1041–1120.

[3] P. Bougerol and J. Lacroix, *Products of random matrices with applications to Schrödinger operators*, Progr. Probab. Statist., Birkhäuser Boston, Inc.

[4] J. Bourgain, A. Gamburd and P. Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. Math. **179** (2010), 559–644.

[5] E. Breuillard and A. Gamburd, *Strong uniform expansion in* SL$(2,p)$, Geom. Funct. Anal. **20** (2010), 1201–1209.

[6] E. Breuillard and P. P. Varjú, *Irreducibility of random polynomials of large degree*, Acta Math. **223** (2019), 195–249.

[7] S. Eberhard, *The characteristic polynomial of a random matrix*, Combinatorica **42** (2022), 491–527.

[8] A. Ferber, V. Jain, A. Sah and M. Sawhney, *Random symmetric matrices: rank distribution and irreducibility of the characteristic polynomial*, Math. Proc. Cambridge Philos. Soc. **174** (2023), 1–14.

[9] A. S. Golsefidy and S. Srinivas, *Random walk on group extensions*, Trans. Amer. Math. Soc. **378** (2025), 2363–2428.

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

[11] J. Kahn, J. Komlós and E. Szemerédi, *On the probability that a random* ±1 *matrix is singular*, J. Amer. Math. Soc. **8** (1995), 223–240.

[12] K. Tikhomirov, *Singularity of random Bernoulli matrices*, Ann. Math. **191** (2020), 593–634.

Stratification of exponential sums and commuting matrices

Tim Browning
(joint work with Will Sawin and Victor Wang)

The main goal is to count integral points of height $\le T$, as $T \to \infty$, on the *commuting variety*

$$\mathsf{C}_n = \{(X,Y) \in \mathsf{M}_n(\mathbb{C})^2 : XY = YX\},$$

viewed as an affine variety in $\mathsf{M}_n(\mathbb{C})^2 \cong \mathbb{C}^{2n^2}$, where M_n is the scheme of $n \times n$ matrices. Thus we are interested in the behaviour of the counting function

$$N(T) = \#\{(X,Y) \in \mathsf{M}_n(\mathbb{Z})^2 : |X|, |Y| \le T,\ XY = YX\},$$

as $T \to \infty$, where $|X|$ denotes the maximum modulus of the entries in a matrix $X \in \mathsf{M}_n(\mathbb{Z})$. Over any finite field k of cardinality q, it is possible to write down an exact formula for $\#\mathsf{C}_n(k)$. This is done in work of Feit and Fine [1] and leads to the asymptotic result $\#\mathsf{C}_n(k) = q^{n^2+n}(1+o(1))$, as $q \to \infty$. In particular, this is consistent with the well-known fact that C_n is an irreducible algebraic variety of dimension n^2+n.

Returning to the counting function $N(T)$, we have the obvious lower bound

$$N(T) \ge \#\{(X,Y) \in \mathsf{M}_n(\mathbb{Z}) \times \mathbb{Z}I_n : |X|, |Y| \le T\} \gg T^{n^2+1},$$

since a scalar matrix commutes with any matrix. In this way we are led to make the following conjecture.

Conjecture. *For any $\varepsilon > 0$ we have $N(T) \ll_\varepsilon T^{n^2+1+\varepsilon}$.*

For $n \le 3$ it is possible to prove the conjectured bound by examining the underlying system of n^2 quadratic equations in $2n^2$ variables, but it seems too complicated to do so when n is large. The following is our main result.

Theorem 1. *We have $N(T) \ll_\varepsilon T^{n^2+2-2/(n+1)}$.*

Our proof uses reduction modulo a suitably chosen prime p, together with Poisson summation and the analysis of exponential sums over finite fields. For the latter we invoke a stratification result of Fouvry and Katz [2], together with the following flatness result, which we also prove.

Theorem 2. *Let* V_n *be the subscheme of matrices in* M_n *with trace* 0*. The map*

$$[\cdot,\cdot] : \mathsf{M}_n(\mathbb{C})^2 \to \mathsf{V}_n(\mathbb{C}), \quad (X,Y) \mapsto XY - YX$$

is flat over the open set $\mathsf{V}_n(\mathbb{C}) \setminus \{0\}$.

References

[1] W. Feit and N. J. Fine, Pairs of commuting matrices over a finite field. *Duke Math. J.* **27** (1960), 91–94.

[2] E. Fouvry and N. Katz, A general stratification theorem for exponential sums, and applications. *J. reine angew. Math.* **540** (2001), 115–166.

A nonabelian circle method

Victor Y. Wang

(joint work with Nuno Arala, Jayce R. Getz, Jiaqi Hou, Chun-Hsien Hsu, and Huajie Li)

Let $M_d(R)$ be the set of $d \times d$ matrices with entries in R. Counting solutions to Diophantine equations in matrices or algebras involves a diverse array of methods, based on the level of symmetry present in a given problem. In the most symmetric situations, dynamical methods tend to work well. For example, Eskin–Mozes–Shah [1, 2] gave an asymptotic formula as $T \to \infty$ for

$$\#\{X \in M_d(\mathbb{Z}) : X^d = kI_d,\ |X|^2 := \sum_{1\le i,j\le d} X_{ij}^2 \le T^2\}$$

for $k \in \mathbb{Z}$ such that $t^d - k \in \mathbb{Z}[t]$ is irreducible. The variety $X^d = kI_d$ carries an action of $\mathrm{GL}_d(\mathbb{Z})$ by conjugation; in fact, its integral points break up into finitely many orbits for this action. Equidistribution of the discrete sets $\{\frac{X}{k^{1/d}}\}$ in an appropriate real space, as $|k| \to \infty$, was established by Einsiedler–Lindenstrauss–Michel–Venkatesh [3, Corollary 3.5] when $d = 3$. The results of the aforementioned papers are more general, but we have singled out $X^d = kI_d$ for simplicity.

A less symmetric example appeared in Tim's talk, concerning the paper [4]. The variety $XY = YX$, for $d \times d$ matrices X and Y, is conjugation-invariant, but for dimension reasons the number of orbits is infinite. Nonetheless, this conjugation symmetry is an essential ingredient in the inductive procedure of [4].

Another less symmetric example is given by the application of a nonabelian circle method in Arala–Getz–Hou–Hsu–Li–W. [5]. Let $D/\mathbb{Q}$ be a quaternion algebra ramified at $S \supset \{2, \infty\}$. Fix a maximal order $\mathcal{O}_D \subset D$ and a function $w \in C_c^\infty(D^n \otimes \mathbb{R})$, where $n \ge 8$. Then for $\upsilon = (\upsilon_1, \dots, \upsilon_n) \in \{\pm 1\}^n$ and $T \ge 1$,

$$\sum_{x\in\mathcal{O}_D^n:\, \upsilon_1 x_1^2+\cdots+\upsilon_n x_n^2=0} w(x/T) = c_{\upsilon,w} T^{4n-8} + O_{w,\epsilon}(T^{3n+\epsilon}).$$

This gives an asymptotic formula for $n \geq 9$. Moreover, we expect that there is a secondary term $c'_{v,w}T^{3n-2}$ coming from the locus

$$\operatorname{tr}(x_1) = \cdots = \operatorname{tr}(x_n) = 0,$$

on which the quaternions x_i^2 collapse into scalars (by Cayley–Hamilton).

One could take Hamilton's classical quaternions $D = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$, with

$$i^2 = j^2 = k^2 = ijk = -1 \quad \text{(Broome Bridge, Dublin, 1843)},$$

and $\mathcal{O}_D = \frac{1+i+j+k}{2}\mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + k\mathbb{Z}$ the Hurwitz quaternions (1919).

Classically, the equation

$$v_1x_1^2 + \cdots + v_nx_n^2 = 0$$

may be viewed as a system of 4 quadratic equations in $4n$ integer variables, upon choosing a $\mathbb{Z}$-basis of $\mathcal{O}_D$. This system has a large singular locus in the various senses of Birch [6], Myerson [7], Hochfilzer [8], and Yamagishi [9]. Thus, prior to [5], an asymptotic formula was available for $n \geq 17$, thanks to [7]. In [5], we do better using the particular structure of quaternions.

The methods of [5] are partly automorphic, for main term calculations, and partly geometric, for error term calculations. To illustrate the geometric ideas, one may consider a nonabelian level of distribution, which is simpler (and easier to generalize) than a nonabelian circle method. In either setting, our results are governed by nonabelian Weyl sums.

Let $d \in \{2,3\}$ and $r \in M_d(\mathbb{Z})$, with $|\det(r)|$ prime and $|\det(r)| \asymp |r|^d$. Let $T \asymp |r| > 0$. Work in progress of Arala–W. (2025+) shows that if $w \in C_c^\infty(M_d(\mathbb{R}))$ and $a \in M_d(\mathbb{Z}) \setminus M_d(\mathbb{Z})r$, then

$$\Sigma_T(ar^{-1}) := \sum_{x \in M_d(\mathbb{Z})} w(x/T) \exp(2\pi i \operatorname{tr}(ar^{-1}x^2)) \ll_{w,\epsilon} T^{d^2 - \frac{d}{2} + \epsilon}.$$

Averaging over $a \in M_d(\mathbb{Z})/M_d(\mathbb{Z})r$ (which is a discrete version of the circle method) shows that if $w \in C_c^\infty(M_d(\mathbb{R})^n)$ and $b \in M_d(\mathbb{Z})$, then

$$\sum_{\substack{x \in M_d(\mathbb{Z})^n \\ x_1^2 + \cdots + x_n^2 - b \in rM_d(\mathbb{Z})}} w(x/T) = \frac{c_w T^{d^2 n}}{|\det(r)|^d} + O_{n,w,\epsilon}(T^{(d^2 - \frac{d}{2})n + \epsilon}).$$

This gives an asymptotic formula for $n \geq 2d+1$. If $d = 2$, then $(d^2 - \frac{d}{2})n = 3n$, matching the error term for the circle method in [5].

Let $N = |\det(r)| \asymp |r|^d \asymp T^d$. We have something like

$$\Sigma_T(ar^{-1}) \ll \sum_{|c| \leq N/T} T^{d^2} |S_{a,r}(c)|$$

by Poisson summation in $M_d(\mathbb{Z}/N\mathbb{Z}) \times M_d(\mathbb{R})$, where

$$S_{a,r}(c) = \frac{1}{N^{d^2}} \sum_{x \in M_d(\mathbb{Z}/N\mathbb{Z})} \exp(2\pi i \frac{\operatorname{tr}(a\operatorname{adj}(r)x^2 + cx)}{\det(r)}),$$

where $\operatorname{adj}(r)r = \det(r)$. In general, the shift $x \mapsto x + ry$ acts nontrivially on the summand (unless we are in the abelian case $d = 1$), but averaging over $y \in M_d(\mathbb{Z})$ shows that if $S_{a,r}(c) \neq 0$, then c lies in the lattice $\Lambda_{a,r}(1)$, where

$$\begin{aligned}\Lambda_{a,r}(K) := \{c \in M_d(\mathbb{Z}) : \exists x \in M_d(\mathbb{Z}),\\ a\operatorname{adj}(r)xr + cr \in NM_d(\mathbb{Z}),\ \operatorname{tr}(2a\operatorname{adj}(r)x + c) \in K\mathbb{Z}\}.\end{aligned}$$

Moreover, one can bound $|S_{a,r}(c)|$ in terms of N and the largest integer $K \mid N$ for which $c \in \Lambda_{a,r}(K)$. After estimating $\#\{c \in \Lambda_{a,r}(K) : |c| \leq N/T\}$ using the geometry of numbers, the desired bound on $\Sigma_T(ar^{-1})$ eventually follows.

The lattice $\Lambda_{a,r}(K)$ has $d^2 \in \{4, 9\}$ successive minima, which can be difficult to control uniformly. One way we control these successive minima is via repulsion arguments. For $d = 3$ we use duality (morally, a second Poisson summation!) and an eigenvalue repulsion argument.

Our results likely only scratch the surface of the subject. Many hypotheses may be removable and many generalizations may be possible.

References

[1] A. Eskin, S. Mozes and N. Shah, *Unipotent flows and counting lattice points on homogeneous varieties*, Ann. of Math. (2) **143** (1996), no. 2, 253–299.

[2] N. Shah, *Counting integral matrices with a given characteristic polynomial*, Sankhyā Ser. A **62** (2000), no. 3, 386–412.

[3] M. Einsiedler, E. Lindenstrauss, P. Michel and A. Venkatesh, *Distribution of periodic torus orbits and Duke's theorem for cubic fields*, Ann. of Math. (2) **173** (2011), no. 2, 815–885.

[4] T. Browning, W. Sawin and V. Wang, *Pairs of commuting integer matrices*, Math. Ann. **393** (2025), no. 2, 1863–1880.

[5] N. Arala, J. Getz, J. Hou, C-H. Hsu, H. Li and V. Wang, *A nonabelian circle method*, arXiv preprint arXiv:2407.11804 (2024).

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

[7] S. Rydin Myerson, *Quadratic forms and systems of forms in many variables*, Invent. Math. **213** (2018), no. 1, 205–235.

[8] L. Hochfilzer, *Systems of bihomogeneous forms of small bidegree*, Acta Arith. **213** (2024), no. 4, 325–368.

[9] S. Yamagishi, *Birch's theorem on forms in many variables with a Hessian condition*, Acta Arith. **221** (2025), no. 2, 141–151.

Moments, vanishing and large values of *L*-functions in thin families

Igor E. Shparlinski

(joint work with Pranendu Darbar, Bryce Kerr, Marc Munsch)

Motivation and set-up: A classical problem in analytic number theory is to understand the distribution of values of Dirichlet L-functions $L(s,\chi)$ for $\chi \in \mathcal{X}_p$, where $\mathcal{X}_p$ is the group of multiplicative characters of $\mathbb{F}_p^*$ for a prime p. In particular, a lot of attention has been devoted to the moments

$$\mathfrak{M}_\nu(s,p) = \frac{1}{p-1} \sum_{\chi \in \mathcal{X}_p} |L(s,\chi)|^\nu,$$

where $\mathcal{X}_p$ is the group of multiplicative characters of $\mathbb{F}_p^*$ for a prime p. Moreover, the values $L(1,\chi)$ and $L(1/2,\chi)$ are of special interest.

While the ultimate goal of understanding individual values of $L(s,\chi)$ remains quite elusive, it is natural to study L-function for thin subsets of $\mathcal{X}_p$. This point of view "interpolates" between pointwise results and results with full averaging over $\mathcal{X}_p$. Here, given an integer $m \ge 1$ with $m \mid p-1$ and a multiplicative subgroup $\mathcal{G}_m \subseteq \mathbb{F}_p^*$ of index m we investigate $L(s,\chi)$ for $\chi \in \mathcal{X}_{p,m}$, where $\mathcal{X}_{p,m}$ is the subgroup of $\mathcal{X}_p$ consisting of characters which are trivial on $\mathcal{G}_m$.

In particular, we are interested in the moments

$$\mathfrak{M}_\nu(s,p,m) = \frac{1}{m}\sum_{\chi\in\mathcal{X}_{p,m}} |L(s,\chi)|^\nu.$$

We remark that similar averages over subgroups $\mathcal{X}_{p,m}$ of fixed index

$$d = (p-1)/m,$$

have recently been studied by Fouvry, Kowalski and Michel [4]. Here we obtain stronger and more uniform versions of some results from [4], which hold for subgroups of optimally large index, see Remark 2 below.

Moments of $L(1,\chi)$: First we obtain the following asymptotic formula, which extends the result of [8] to the optimal range. We also define

$$a(k) = \sum_{n=1}^{\infty} \frac{\tau_k^2(n)}{n^2},$$

where $\tau_k(n) = \#\{(n_1,\ldots,n_s)\in\mathbb{N} :\ n_1\cdots n_k = n\}$ is the k-fold divisor function.

Theorem 1 (Munsch & Shparlinski [10]). *Let k be a fixed integer and let $\kappa < 1$ be an arbitrary constant. For any $m \mid p-1$, we have*

$$\mathfrak{M}_{2k}(1,p,m), = a(k) + O\left(p^{-\kappa/\varphi(d)} + p^{-1/4+o(1)}\right).$$

Remark 2. *We see that Theorem 1 is nontrivial provided that*

$$\varphi(d) = o(\log p), \tag{1}$$

in which case we have

$$\mathfrak{M}_{2k}(1,p,m) = a(k) + o(1), \qquad \text{as } p\to\infty. \tag{2}$$

In fact the range (1) *is the best we can hope even for $k=1$. Indeed, by* [8, Theorem 5.4] *and assuming that there are infinitely many Mersenne primes $p = 2^d-1$, the asymptotic formula* (2) *does not hold in the range $\varphi(d) = d-1 \asymp \log p$.*

However, for almost all primes p, the range (1) can be significantly extended. A consequence of a more general and flexible result, we have:

Theorem 3 (Munsch & Shparlinski [10]). *Let $0<\varepsilon<1$ and let an integer $k\ge 1$ be fixed. For a sufficiently large Q, for any d such that $3\le d\le p^{1/2-\varepsilon}$, we have,*

$$\mathfrak{M}_{2k}(1,p,m) = a(k) + o(1), \qquad \text{as } Q\to\infty,$$

for all except at most $Q^{1-\varepsilon}$ primes $p\in[Q,2Q]$.

Moments and non-vanishing of $L(1/2,\chi)$: At the central point $s = 1/2$, we have nontrivial results only for the second and fourth moments. Nevertheless, this yileds new non-vanishing results over thin subgroups. Let $\Gamma(x)$ denote the standard Γ-function and let $\gamma = 0.57721\ldots$ denote the *Euler–Mascheroni constant.*

Theorem 4 (Munsch & Shparlinski [10])**.** *Let $\kappa < 1/2$. Then for any $m \mid p-1$,*

$$\mathfrak{M}_2(1/2,p,m) = \log\left(\frac{p}{\pi}\right) + 2\gamma + \frac{\Gamma'}{\Gamma}\left(\frac{1}{4}\right) + O\left(p^{-\kappa/\varphi(d)}\log p + p^{-1/8+o(1)}\right).$$

To formulate our result, given a prime p and $\lambda \in \mathbb{Z}$ with $\gcd(p,\lambda) = 1$, we define

$$\rho(\lambda,p) = \min\{rs:\ (r,s) \in \mathbb{N}^2 \setminus \{(0,0)\},\ r \equiv \lambda s \bmod p\},$$

and set

$$\vartheta(p,m) = \min_{\lambda \in \mathcal{G}_m \setminus \{1\}} \rho(\lambda,p).$$

Theorem 5 (Munsch & Shparlinski [10])**.** *For any $\varepsilon > 0$ there $c(\varepsilon) > 0$ which depends only on ε such that for any d with $1 \le d \le p^{1/8-\varepsilon}$, we have*

$$\frac{1}{m}\sum_{\chi \in \mathcal{X}_{p,m};\ L(1/2,\chi)\neq 0} 1 \ge c(\varepsilon)\frac{\log \vartheta(p,m)}{\log p}.$$

For almost all primes, our method produces the following result.

Theorem 6 (Munsch & Shparlinski [10])**.** *Let $Q \ge 2$ be sufficiently large. For any $\varepsilon > 0$ there $c(\varepsilon) > 0$ which depends only on ε such that for all except at most $Q^{1/2}$ primes $p \in [Q,2Q]$, for any d with $1 \le d \le p^{1/6-\varepsilon}$, we have*

$$\frac{1}{m}\sum_{\chi \in \mathcal{X}_{p,m};\ L(1/2,\chi)\neq 0} 1 \ge c(\varepsilon).$$

Extreme values and zero-density theorems: In work in progress [3] we obtain lower bounds on extreme values of $L(s,\chi)$, with $\Re s \in [1/2,1]$ which in some cases become of the same shape as those of Bondarenko & Seip [1]. In turn, some of these results rely on a new zero-density estimate.

Let $N(\sigma,T,\chi)$ be the number of zeros of $L(s,\chi)$ with $\Re s \ge \sigma$ and $|\Im s| \le T$.

Theorem 7 (Darbar, Kerr, Munsch & Shparlinski [3])**.** *Let $\sigma > 1/2$ be fixed. Then for any $T \le (\log p)^{O(1)}$*

$$\sum_{\chi \in \mathcal{X}_{p,m}} N(\sigma,T;\chi) \le p^{o(1)} \begin{cases} m^{(7-6\sigma)/(6-4\sigma)} & \textit{if } m \ge q^{2/3}, \\ m^{(4-3\sigma)/(6-4\sigma)} p^{(1-\sigma)/(3-2\sigma)} & \textit{if } m < q^{2/3}. \end{cases}$$

We recall the classical bound $N(1,T;\chi) \ll T\log(qT) + \log q$ see, for example, [5, Theorem 5.8]. Hence, we trivially have

$$\sum_{\chi \in \mathcal{X}_{p,m}} N(\sigma,T;\chi) \le mp^{o(1)}, \tag{3}$$

in the range of T of Theorem 7. On the other hand, one easily verifies that for $\sigma > 1/2$ we have $(7-6\sigma)/(6-4\sigma) < 1$. Hence, if $m \ge p^{2/3}$, Theorem 7 is nontrivial for any $\sigma(1/2,1)$. Similarly, for $p^{2/3} > m \geq p^{\eta}$ with some fixed $\eta > 0$ Theorem 7 improves (3) as long as $\sigma > 1 - \eta/(2-\eta)$.

Underlying tools and further applications: The quantity $\rho(\lambda, p)$ and its higher-dimensional analogues are well-studied in the context of the theory of pseudo-random generators and numerical integration; we refer for more information to the work of Korobov [6, 7] and Niederreiter [11]. As in our case, for these applications it is important to have good lower bounds on these quantities.

Our results for almost all primes are also based on some results [10] of additive combinatorics flavour about expansion of product sets of subsets of sets of Farey fraction of order Q, extending those of [2, 13].

Furthermore, Theorem 7, also depend on the following bound on average values of character sums, improving and generalising that of Montgomery [9] on moments of character sums.

Theorem 8 (Darbar, Kerr, Munsch & Shparlinski [3])**.** *Let $\mathcal{A} \subseteq \mathcal{X}_p$ be a set of cardinality $A = \#\mathcal{A}$ of multiplicative characters with the product set $\mathcal{B} = \mathcal{A} \cdot \mathcal{A}$ satisfying $\#\mathcal{B} \leq KA$ for some $K \geq 1$. Then for a positive integer $N \leq p$ and complex coefficients $|\alpha_n| \leq 1$, $1 \leq n \leq N$, we have*

$$\frac{1}{A} \sum_{\chi \in \mathcal{A}} \left| \sum_{n=1}^{N} \alpha_n \chi(n) \right| \leq K^{1/2} \left(N^{1/2} + A^{-1/2} N + A^{-3/8} N^{1/2} p^{1/4} \right) p^{o(1)}.$$

Besides application to zero-density estimates, Theorem 8 has also been used to establish unconditionally a GRH-conditional result of Rudnick & Zaharescu [12] on pair correlation of small powers of primitive roots.

References

[1] A. Bondarenko and K. Seip, *Extreme values of the Riemann zeta function and its argument*, Math. Ann. **372** (2018), 999–1015.

[2] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Product sets of rationals, multiplicative translates of subgroups in residue rings, and fixed points of the discrete logarithm', *Int. Math. Res. Not.*, **2008** (2008), Article ID rnn090.

[3] P. Darbar, B. Kerr, M. Munsch and I. E. Shparlinski, *Large values of $L(\sigma, \chi)$ for subgroups of characters*, In progress.

[4] É. Fouvry, E. Kowalski and Ph. Michel, *Toroidal families and averages of L-functions, I*, Acta Arith. **214** (2024), 109–142.

[5] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[6] N. M. Korobov, *Number-theoretical methods in approximate analysis*, Fizmatgiz, Moscow, 1963 (in Russian).

[7] N. M. Korobov, *Some problems of the theory of Diophantine approximations*, Russian Mathematical Surveys, **22** (1967), no. 3, 83–118 (translated from Uspehi Mat. Nauk).

[8] S. Louboutin and M. Munsch, *Mean square values of L-functions over subgroups for non primitive characters, Dedekind sums and bounds on relative class numbers*, Canad. J. Math. **75** (2023), 1711–1743.

[9] H. L. Montgomery, *Distribution of small powers of a primitive root*, Advances in Number Theory, Clarendon Press, Oxford, 1993, 137–149.

[10] M. Munsch and I. E. Shparlinski, *Moments and non-vanishing of L-functions over thin subgroups*, Preprint, 2023, available from `https://arxiv.org/abs/2309.10207`.

[11] H. Niederreiter, *Pseudo-random numbers and optimal coefficients*, Adv. Math. **26** (1977), 99–181.

[12] Z. Rudnick and A. Zaharescu, *The distribution of spacings between small powers of a primitive root*, Israel J. Math. **120** (2000), 271–287.

[13] Y. N. Shteinikov, *On the product sets of rational numbers*, Proc. Steklov Inst. Math. **296** (2017), 243–250.

Character sums over polynomial values

Étienne Fouvry
(joint work with Igor Shparlinski, Ping Xi)

Let $p \geq 3$. We identify the set of integers $\{0, \cdots, p-1\}$ with $\mathbb{F}_p$. Let P be a monic polynomial of $\mathbb{F}_p[X]$, with degree $d \geq 1$, factorized into the product of irreducible monic polynomials as $P(X) = P_1(X) \cdots P_r(X)$. We define the *geometric Möbius function* μ_p by the formula

$$\mu_p(P) := \begin{cases} 0 & \text{if } P_i = P_j \text{ for some } 1 \leq i < j \leq r, \\ (-1)^r & \text{otherwise.} \end{cases}$$

We aim at proving oscillations of $\mu_p(P)$ when all of the coefficients of P belong to a small interval, when compared with p. A first typical result is

Theorem 1. *(*[3]*) Let d and k be coprime integers, such that $d > k \geq 1$, and $d \geq 3$. Then, for very $\delta > 0$, there exists $\varepsilon > 0$, such that, uniformly for A and $B \geq p^{d/(2d+1)+\delta}$, one has the inequality*

$$\sum_{0 \leq a \leq A} \sum_{0 \leq b \leq B} \mu_p(X^d + aX^k + b) = O\left(ABp^{-\varepsilon}\right).$$

The important fact is the inequality $d/(2d+1) < 1/2$ which means that we overcome Pólya–Vinogradov barrier.

The function μ_p is associated with the Legendre symbol via a consequence of a theorem of Stickelberger (see for instance [1]). More precisely let disc P be the discriminant of the polynomial P and let d be its degree. We then have the equality

$$\mu_p(P) = (-1)^d \left(\frac{\text{disc } P}{p}\right).$$

Idea of the proof of Theorem 1. The trinomial $X^d + aX^k + b$ has a rather simple expression of its discriminant

$$\text{disc}\left(X^d + aX^k + b\right) = (-1)^{\frac{d(d-1)}{2}} a^{k-1} \left\{d^d a^{d-k} + (-1)^{d+1}(d-k)^{d-k} k^k b^d\right\}.$$

So, in order to prove Theorem 1, we are naturally led to study the more general sum

$$\mathfrak{S}_\chi(\mathcal{A}, \mathcal{B}; p) := \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(a^k b^\ell (sa^m + tb^n))$$

where

- χ is a multiplicative character modulo p with order $h > 1$,
- $\mathcal{A}$ and $\mathcal{B}$ are intervals of the form $[A_0+1, \cdots, A_0+A]$ and $[B_0+1, \cdots, B_0+B]$,
- s and t are integers that p does not divide st,
- k, ℓ, m and n are integers such that $0 \leq k, \ell < h$, $(m,n) = 1$ and $mn > 0$.

We prove the following

Theorem 2. *([3]) We adopt the above notations and we assume the above hypotheses. Then, for every fixed integer $r \geq 2$, for every A and B such that*

$$B^{n/m}A^{-1} \leq p^{(n-m)/(2mr)} \text{ and } B \geq 4p^{1/(2r)},$$

we have the inequality

$$|\mathfrak{S}_\chi(\mathcal{A}, \mathcal{B}; p)| \leq AB \left(\frac{p}{AB^{1+(1/|m|)}}\right)^{1/2r} p^{(m+1)/(4mr^2)+o(1)},$$

as p tends to infinity. The o–function only depends on the integers h, k, ℓ, m, n, r, s and t.

Remark that m and n can both be negative. If it is the case, then playing with the denominators, we are reduced to consider the cases where m and n are both positive.

We apply several classical procedures to study $\mathfrak{S}_\chi(\mathcal{A}, \mathcal{B}; p)$:

• a shift *à la carte* of the variables a and b

$$(a, b) \mapsto (a + uw^n, b + vw^m),$$

where $u \sim U$, $v \sim V$ and $w \sim W$, the parameters U, V and W are at our disposal and satisfy the relations

$$UW^n = A/4 \text{ and } VW^m = B/4,$$

• Hölder's inequality.

Applying these procedures, we arrive at the crucial sum

$$S := \sum_{(\mathbf{u},\mathbf{v})} \Sigma(\mathbf{u}, \mathbf{v}) \tag{1}$$

where

$$\Sigma(\mathbf{u}, \mathbf{v}) := \sum_{x,y=1}^{p} \prod_{j=1}^{r} \chi\left((x+u_j)^k(y+v_j)^\ell(s(x+u_j)^m + t(y+v_j)^n)\right) \times \overline{\chi}\left((x+u_{r+j})^k(y+v_{r+j})^\ell(s(x+u_{r+j})^m + t(y+v_{r+j})^n)\right),$$

where the sum (1) is made over the vectors of translation

$$(\mathbf{u}, \mathbf{v}) = (u_1, \cdots, u_r, u_{r+1}, \cdots, u_{2r}, v_1, \cdots, v_r, v_{r+1}, \cdots, v_{2r}).$$

These vectors belong to a space of dimension $4r$ and their coordinates satisfy $u_i \sim U$ and $v_i \sim V$. Denote by $\mathcal{B}$ the set of these $(\mathbf{u}, \mathbf{v})$. The cardinality of $\mathcal{B}$ is about $U^{2r}V^{2r}$. A trivial bound is $|\Sigma(\mathbf{u}, \mathbf{v})| \leq p^2$ and the square root cancellation for this sum would be $|\Sigma(\mathbf{u}, \mathbf{v})| \ll p$. An individual study of the bidimensional sum

$\Sigma(\mathbf{u},\mathbf{v})$ is very intricate. However we benefit from the fact that we are summing over $(\mathbf{u},\mathbf{v})$ as follows. Introduce the following sum

$$\Lambda := \sum_{x,y=1}^{p} \prod_{j=1}^{2r} \chi_i \left(x^k y^\ell (sx^m + ty^n)\right)$$

with $\chi_1 = \chi_2 = \cdots = \chi_r = \chi$ and $\chi_{r+1} = \chi_{r+2} = \cdots = \chi_{2r} = \overline{\chi}$. Then $\Sigma(\mathbf{u},\mathbf{v})$ appears to be a *perturbation* of Λ through a translation of the variable (x,y) with the vector $(\mathbf{u},\mathbf{v})$.

In an important paper, J. Xu [4] analyzes the impact of such a general translation to a sum of multiplicative characters over rational functions in several variables. Xu's result appears to be an analogue of the stratification theory in the context of additive characters (see for instance [2]). Thanks to [4, Theorem 1.1] we deduce the bound

$$S \ll \sharp(\mathcal{X}_2 \cap \mathcal{B})p^2 + \sharp(\mathcal{X}_1 \cap \mathcal{B})p^{\frac{3}{2}} + \sharp(\mathcal{X}_0 \cap \mathcal{B})p, \tag{2}$$

where $\mathcal{X}_2$, $\mathcal{X}_1$ and $\mathcal{X}_0$ are some varieties with dimensions $4r$, $3r+1$ and $2r$. To continue the exposition, we suppose that $U \geq V$. By bounding the number of points of the variety $\mathcal{X}_j$ which also lie in the box $\mathcal{B}$, we transform the inequality (2) into

$$S \ll p^2 U^{2r} + p^{\frac{3}{2}} U^{2r} V^{r+1} + p(UV)^{2r}, \tag{3}$$

The choice of the parameters V is $V = p^{1/(2r)}$, thus the first and third terms of (3) are equal. This leads to the bound of Theorem 2.

However, in order to apply [4, Theorem 1.1] we must firstly check that the polynomial in two variables X and Y, defined by

$$F(X,Y) = X^k Y^\ell (sX^m + tY^n),$$

is not divisible by the h–power of a non constant polynomial. This is trivial since $0 \leq k$, $\ell < h$ and since $st \not\equiv 0 \bmod p$. Secondly, we must check that the cardinality of $(x,y) \in \overline{\mathbb{F}_p}^2$, such that $F(X+x, Y+y) = F(X,Y)$ is finite, for sufficiently large p. Actually, the set of such (x,y) is reduced to $\{(0,0)\}$. This is easy to prove by considering the equality $F(-x+x, Y+y) = F(-x,Y) = 0$, for instance.

A natural question is to generalize Theorem 1 to other families of polynomials. This is a work in progress.

References

[1] L. Carlitz, *A theorem of Stickelberger*, Math. Scand. **1** (1953), 82–84.

[2] E. Fouvry & N. Katz, *A general stratification theorem for exponential sums, and applications,* J. Reine Angew. Math. **540** (2001), 115–166.

[3] E. Fouvry, I. Shparlinski & P. Xi, *Character sums with discriminants and sums of geometric Möbius functions,* (in preparation).

[4] J. Xu, *Stratification for multiplicative character sums*, Int. Math. Res. Not. IMRN 2020, **10** (2020), 2881–2917.

Irreducibility of random Fekete polynomials

Max Wenqiang Xu
(joint work with Péter P. Varjú)

The study of the irreducibility of random polynomials has been very active. The breakthrough work of Breuillard and Varju [1] showed that, conditional on GRH, the ±1 random polynomial is irreducible with high probability as the degree $d \to +\infty$. In this talk, we study a more arithmetic flavor variant of the question. Our motivation is to study the irreducibility of Fekete polynomials, whose coefficients are multiplicative.

We first prove the irreducibility for the natural random model of Fekete polynomial. Let $X(n)$ be a random multiplicative function taking values $\{1,-1\}$. Namely, for prime p, $X(p) \sim U(\{1,-1\})$ and $X(n)$ is defined multiplicatively. Then the natural random Fekete polynomial would be

$$F_d(t) = \sum_{i=1}^{d} X(i)t^i.$$

Theorem 1. *Conditional on GRH,*

$$\mathbb{P}[\frac{F_d(t)}{t} \textit{ is irreducible over } \mathbb{Z}] = 1 - O(d^{-1/2+\epsilon}).$$

We can also deduce a "deterministic" version if we average enough number of Fekete polynomials. Define

$$F_{d,p}(t) = \sum_{1 \le i \le d} \chi_p(i)t^i.$$

Theorem 2. *Conditional on GRH, if we uniformly at random choose $p \in [d+1, d^4 2^{2\pi(d)}]$, then*

$$\mathbb{P}[\frac{F_{d,p}(t)}{t} \textit{ is irreducible over } \mathbb{Z}] = 1 - O(d^{-1/2+\epsilon}).$$

References

[1] E. Breuillard and P. P. Varj´u, *Irreducibility of random polynomials of large degree*, Acta Math. **223** no.2, 195–249.

Rational points near space curves

Niclas Technau
(joint work with Mingfeng Chen, Andreas Seeger, Rajula Srivastava)

Many problems in number theory involve counting rational points near manifolds. For a well-written introduction to the subject, see V. Beresnevich [1] and J.-J. Huang [3]. This talk is based on work in progress with the authors mentioned in the sub-title. In a nutshell, we investigate the density of rational points with the same denominator which are in a neighbourhood of a space curve. Of course, the thickness of the neighbourhood in terms of the (naive) height of the rational points to be counted plays a key role. To detail this precisely, let

$$\mathcal{C} \subseteq \mathbb{R}^3$$

be a compact C^∞-curve. (The smoothness assumption can be reduced but we shall only report on smooth curves for the ease of the exposition.) Let $Q \geq 1$ be large, and $\delta \in [0,1]$ be small. We define the dyadic counting function

$$N_{\mathcal{C}}(\delta, Q) := \#\{(\mathbf{p}, q) \in \mathbb{Z}^3 \times \mathbb{N} : Q \leq q \leq 2Q,\ \operatorname{dist}(\mathcal{C}, \mathbf{p}/q) \leq \delta/Q\}$$

where $\operatorname{dist}(\mathcal{C}, \mathbf{y})$ denotes the distance of the point $\mathbf{y} \in \mathbb{R}^3$ to $\mathcal{C}$ with respect to the Euclidean norm on $\mathbb{R}^3$. Our objective is to determine the magnitude of $N_{\mathcal{C}}(\delta, Q)$, up to multiplicative constants. Without loss of generality, we can assume $\mathcal{C}$ is the image of a regular, injective C^∞-map

$$\boldsymbol{\gamma} : I \to \mathbb{R}^3$$

where I is a compact interval. A folklore conjecture, based on a straightforward random model, states the following. There is a constant $K = K(\mathcal{C}) > 0$ so that

$$\frac{1}{K}(\delta Q)^2 \leq N_{\mathcal{C}}(\delta, Q) \leq K(\delta Q)^2 \tag{1}$$

for any $Q \geq 1$ and all

$$\delta \in (Q^{\varepsilon - \frac{1}{2}}, 1)$$

provided $\mathcal{C}$ is sufficiently curved. The planar version of this counting problem was solved by R.C. Vaughan and S. Velani [5] around 2006. In $\mathbb{R}^3$, the previously best known result was due to J.-J. Huang [4]. He showed that if

$$\delta \in (Q^{\varepsilon - \frac{1}{5}}, 1),$$

then the folklore conjecture is true under the geometric assumption (2) from below. To avoid that $\mathcal{C}$ is flat, which could cause an over-count and the random model to fail for trivial reasons, one imposes curvature conditions. Let $U \subset \mathbb{R}$ be an open set containing the interval concentric to I but with twice the radius. We assume that $\boldsymbol{\gamma}$ extends to a smooth map on U which satisfies the curvature condition

$$\inf_{t \in I} |\det(\boldsymbol{\gamma}^{(1)}(t),\, \boldsymbol{\gamma}^{(2)}(t),\, \boldsymbol{\gamma}^{(3)}(t))| > 0. \tag{2}$$

Here is our main result. Suppose $\mathcal{C} = \boldsymbol{\gamma}(I)$ satisfies (2). Then, the heuristic (1) holds for all $Q \geq 1$ and

$$\delta \in (Q^{\varepsilon - \frac{1}{3}}, 1).$$

Moreover, we show by a rich class of examples that our range of δ is actually sharp.

References

[1] V. Beresnevich: *Rational points near manifolds and metric Diophantine approximation.* Annals of Mathematics (2012): 187–235.

[2] V. Beresnevich, D. Dickinson, and S. Velani: *Diophantine approximation on planar curves and the distribution of rational points.* Annals of Mathematics (2007): 367–426.

[3] J. J. Huang: *The density of rational points near hypersurfaces.* Duke Math Journal, Vol. 169, No. 11 (2020): 2045–2077.

[4] J.-J. Huang: *Integral points close to a space curve.* Mathematische Annalen, Vol. 374.3, (2019): 1987–2003.

[5] R.C. Vaughan, and S. Velani: *Diophantine approximation on planar curves: the convergence theory.* Inventiones Mathematicae 166.1 (2006): 103–124.

Hilbert properties of varieties

Arno Fehm

Hilbert's irreducibility theorem [12] motivates Serre's definition of thin sets of rational points [18], as well as the Hilbert property by Colliot-Thélène and Sansuc [4], and the weak Hilbert property by Corvaja and Zannier [6]. In this talk I gave a short survey on some of the recent research on these properties, based on a survey paper written jointly with Ariyan Javanpeykar [9].

Let k always be a field of characteristic zero and let X be a k-variety (all varieties geometrically integral and normal) of positive dimension. A set $T \subseteq X(k)$ is **[strongly] thin** if

$$T \subseteq Z(k) \cup \bigcup_{i=1,\dots,r} \pi_i(Y_i(k))$$

for $Z \subsetneq X$ closed and $\pi_i \colon Y_i \to X$ a [ramified] cover with $\deg(\pi_i) > 1$ (here, a *cover* is a finite surjective morphism of k-varieties). The k-variety X has **[W]HP** if $X(k)$ is not [strongly] thin, and **potential [W]HP** if $X_{k'}$ has [W]HP for some finite extension k'/k. The field k is **Hilbertian** if $\mathbb{A}^1_k$ has HP (equivalently, WHP), and Hilbert's irreducibility theorem can be rephrased as saying that number fields are Hilbertian.

If k is a number field and X is smooth projective, Corvaja and Zannier [6] show that X has HP if and only if X has WHP and $X_{\overline{k}}$ is simply connected (a purely geometric property), and they suggest that X might have potential WHP if and only if $X(k')$ is Zariski-dense in X for some finite extension k'/k, which by a conjecture of Campana [3] is predicted to be equivalent to another purely geometric property ("$X_{\bar{k}}$ is special").

The case of curves is well understood by the Mordell–Weil theorem and Faltings's theorem:

Theorem 1. *Let C be a smooth projective curve over k. Assume that k is a number field.*

(1) *C has HP ⇔ C is rational (i.e. $C \cong \mathbb{P}^1_k$).*
(2) *C has WHP ⇔ C is rational or an elliptic curve of positive rank.*

In particular, C has potential HP if and only if $g_C = 0$, and potential WHP if and only if $g_C \leq 1$.

I then summarized some of the recent progress on algebraic groups and surfaces:

Theorem 2. *Let G be a connected algebraic group over k.*

(1) *If k is Hilbertian and G is linear, then G has HP.* [4, 1]

(2) *If k is a number field, then G has potential WHP. More precisely:*
   (a) *G has HP $\Leftrightarrow$ G is linear.* [17, 4, 1]
   (b) *G has WHP $\Leftrightarrow$ $G(k)$ is Zariski-dense in G.* [5, 13, 14]

Theorem 3. *Let X be a smooth projective surface over k of Kodaira dimension $\kappa(X) \in \{-\infty, 0, 1, 2\}$.*

(1) *Suppose that $\kappa(X) < 0$. In this case, $X_{\overline{k}}$ is birational to $\mathbb{P}^1 \times C$ for a smooth projective curve C. In case $g_C = 0$, X is birational to a del Pezzo surface (of degree $d \in \{1, \dots, 9\}$) or to a surface that admits a conic fibration.*
   (a) *If k is a number field, X has potential WHP if and only if $g_C \leq 1$.*
   (b) *If k is a number field, $g_C = 1$ and $X(k)$ is Zariski-dense in X, then X has WHP.*
   (c) *Suppose that k is Hilbertian and X is a del Pezzo surface with $X(k)$ Zariski-dense in X. If X is of degree 1, assume in addition that X admits a conic fibration. Then X has HP.* [19, 8]

(2) *Suppose that $\kappa(X) = 0$. In this case, $X_{\overline{k}}$ is birational to (I) a K3 surface, (II) an Enriques surface, or (III) a surface with an étale cover which is an abelian surface. Suppose that k is a number field.*
   (a) *In cases (II) and (III), X has potential WHP.* [10, 5]
   (b) *In case (I), X has potential HP if $X_{\overline{k}}$ admits two distinct elliptic fibrations.* [11, 7]

Finally, I explained some of the tools that are used in such results, namely going down theorems and fibration theorems:

Theorem 4. *Let $f\colon X \to Z$ be a dominant morphism of k-varieties.*

(1) *If X has [W]HP and f has geometrically irreducible generic fiber, then Z has [W]HP, where in the case of WHP we assume f smooth surjective.* [4, 5, 2]

(2) *If Z has [W]HP and there is a dense open subset $U \subseteq Z$ such that for every $z \in U(k)$ the fiber $f^{-1}(z)$ has HP, then X has [W]HP.* [1, 15]

(3) *If Z has HP and the generic fiber of f has [W]HP, then X has [W]HP, where in the case of WHP we assume X, Z smooth and f smooth proper.* [2, 16]

For more details and full references see [9]. I also advertised Oberwolfach Seminar 2643a on this topic.

References

[1] L. Bary-Soroker, A. Fehm and S. Petersen. On varieties of Hilbert type. *Ann. Inst. Fourier (Grenoble)* 64(5):1893–1901, 2014.

[2] L. Bary-Soroker, A. Fehm and S. Petersen. Hilbert properties under base change in small extensions. arXiv:2312.16219 [math.NT]. To appear in *Ann. Sc. Norm. Super. Pisa Cl. Sci.*, 2025.

[3] F. Campana. Orbifolds, special varieties and classification theory. *Ann. Inst. Fourier (Grenoble)* vol. 54, p. 499–630, 2004.

[4] J.-L. Colliot-Thélène and J.-J. Sansuc. Principal homogeneous spaces under flasque tori: applications. *J. Algebra* 106:148–205, 1987.

[5] P. Corvaja, J. L. Demeio, A. Javanpeykar, D. Lombardo and U. Zannier. On the distribution of rational points on ramified covers of abelian varieties. *Compos. Math.* 158(11):2109–2155, 2022.

[6] P. Corvaja and U. Zannier. On the Hilbert property and the fundamental group of algebraic varieties. *Math. Z.* 286:579–602, 2017.

[7] J. L. Demeio. Elliptic fibrations and the Hilbert property. *Int. Math. Res. Not. IMRN* 2021(13):10260–10277, 2021.

[8] J. Demeio, S. Streeter and R. Winter. Weak weak approximation and the Hilbert property for degree-two del Pezzo surfaces. *Proc. London Math. Soc.* (3) 2024;128:e12601.

[9] A. Fehm and A. Javanpeykar. Hilbert properties of varieties. arXiv:2511.18431 [math.AG], 2025.

[10] D. Gvirtz-Chen and G. Mezzedimi. A Hilbert irreducibility theorem for Enriques surfaces. *Trans. Amer. Math. Soc.* 376(6):3867–3890, 2023.

[11] D. Gvirtz-Chen and G. Mezzedimi. Non-thin rational points for elliptic K3 surfaces. arXiv:2404.06844 [math.AG], 2024.

[12] D. Hilbert. Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten. *J. reine angew. Math.* 110:104–129, 1892.

[13] F. Liu. On Hilbert's irreducibility theorem for linear algebraic groups. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)* 23:1054–1089, 2022.

[14] C. Luger. Products of varieties with many integral points. arXiv:2401.05203 [math.AG]

[15] C. Luger. A mixed fibration theorem for Hilbert irreducibility on non-proper varieties. To appear in *Arch. Math. (Basel)*. arXiv:2410.13741 [math.AG]

[16] S. Petersen. Fibration theorems for varieties with the weak Hilbert property. arXiv:2510.24479 [math.AG], 2025.

[17] J.-J. Sansuc. Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres. *J. reine angew. Math.* 327:12–80, 1981.

[18] J.-P. Serre. *Topics in Galois theory.* Second edition. Springer, 2008.

[19] S. Streeter. Hilbert property for double conic bundles and del Pezzo varieties. *Math. Research Letters* 28(1):271–283, 2021.

Bilinear forms with trace functions

Philippe Michel

(joint work with Etienne Fouvry, Emmanuel Kowalski and Will Sawin)

Given q a prime and $K : \mathbb{Z}/q\mathbb{Z} = \mathbb{F}_q \to \mathbb{C}$ an important problem in analytic number theory is to bound non trivially type I and type II bilinear sums

$$\sum_{m,n\sim M\times N} \alpha_m K(mn), \quad \sum_{m,n\sim M\times N} \alpha_m\beta_n K(mn)$$

the trivial bounds being respectively

$$\|K\|_\infty \|\alpha\| M^{1/2} N,\ \|K\|_\infty \|\alpha\|\|\beta\|(MN)^{1/2}.$$

We consider the case where

$$K(x) = \mathrm{tr}(\mathrm{Frob}_x | V_{\mathcal{F}})$$

is the trace function of an ℓ-adic sheaf pure of weight 0 where it is lisse (and say extended by zero outside its lisse open set) and in the regime where the complexity of the sheaf (in the sense of [6]) $c(\mathcal{F})$ as bounded as $q \to \infty$.

Examples of trace functions include

- Dirichlet characters of $\mathbb{F}_q^\times$: $x \to \chi(x)$
- Additive characters of $\mathbb{F}_q$: $x \to e_q(ax)$
- Kloosterman and hyper-Kloosterman sums: $k \geq 2$

$$\mathrm{Kl}_k(x) = \frac{1}{q^{\frac{k-1}{2}}} \sum_{x_1 \cdot \cdots x_k = x} e_q(x_1 + \cdots + x_k)$$

- Precompositions and product of these by rational fractions

$$x \to K_1(f(x))K_2(g(x))$$

- and much more $\cdots$

A natural barrier (coming from the theory of the Fourier transform) to non-trivial bounds is the *Pólya-Vinogradov (PV) range*

$$M + N \geq q^{1/2} \log q.$$

Starting with Weyl and Burgess (for polynomial phases and Dirichlet characters) that barrier has been passed for various specific classes of trace functions.

In [2] we provide a natural qualitative condition on the geometric monodromy group $G_{\mathcal{F}}$ of $\mathcal{F}$ to pass the PV range.

The sheaf $\mathcal{F}$ is *gallant* if either

(1) its connected component $G^0_{\mathcal{F}}$ is simple.
(2) or $G_{\mathcal{F}}$ is finite and contains a quasi-simple normal subgroup $N_{\mathcal{F}}$ acting irreducibly on $V_{\mathcal{F}}$.

In [2] we provide power saving bounds for the type I and type II bilinear sums below the PV range for trace functions $K = K_{\mathcal{F}}$ associated to gallant sheaves $\mathcal{F}$: we prove that for any $\delta > 0$ one has

$$\sum_{m,n \sim M \times N} \alpha_m K(mn) \ll \|\alpha\| M^{1/2} N q^{-\eta},$$

$$\sum_{m,n \sim M \times N} \alpha_m \beta_n K(mn) \ll \|\alpha\| \|\beta\| (MN)^{1/2} q^{-\eta}$$

as long as $M + N \geq q^\delta$ and

$$MN^2 \geq q^{1+\delta},\ MN \geq q^{3/4+\delta}$$

(respectively); here $\eta = \eta(\delta) > 0$ and the implicit constants depend on δ and the complexity $c(\mathcal{F})$.

The interest of the ”gallant” condition is that it is robust under very natural transformations; For instance, by the work of Katz [3], the hyper-Kloosterman sheaves are gallant as are *their pull-backs* by non-constant rational fractions: if $f(X)$ is not constant the trace function

$$x \mapsto \mathrm{Kl}_k(f(x))$$

is associated with the gallant sheaf $f^*\mathcal{K}\ell_k$. Subsequent works of Katz and collaborators (eg. [4, 5]) provide a broad list ofgallant sheaves of interest to analytic number theory.

In fact these bounds hold for more general bilinear sums with general mononials such as

$$\sum_{m,n\sim M\times N}\alpha_m K(m^bn^c),\quad \sum_{m,n\sim M\times N}\alpha_m\beta_n K(m^bn^c)$$

with $b,c\in\mathbb{Z}-\{0\}$ and more general multilinear sums can be bounded non-trivially below the PV range with the methods of this paper.

The proof starts (possibly after applying Cauchy-Schwarz in the type II case) with the $+ab$ trick of Burgess reduces in obtaining sharp bounds for one or two dimensional sums of products of copies of K shifted by affine maps. From there one continue with relatively "soft" arguments using in addition to [6], the method of moments of J. Xu [7] –generalized to ℓ-sheaves of rank >1 – along with a novel and robust form of the Goursat-Kolchin-Ribet criterion together with a control on the size of the group of projective automorphisms of an ℓ-adic sheaf in terms of its complexity (see [1]).

One motivating application for developing these techniques is the study of cubic mixed moments of Dirichlet L-functions

$$\frac{1}{q-1}\sum_{\chi \mod q} L(1/2,\chi^a)L(1/2,\chi^b)L(1/2,\chi^c)$$

for general triples of non-zero integers (a,b,c). These require to bound bilinear sums in the following exponential sums

$$K_{a,b,c}(x):=\frac{1}{q}\sum_{x_1^ax_2^bx_3^c=x} e_q(x_1+x_2+x_3)$$

which are related to hypergeometric sums in $|a|+|b|+|c|$ variables and are gallant for most triples (a,b,c) from the works of Katz mentionned above.

In a similar vein F. Berta and S. zur Verth have used some of these methods along with the mollification method to show that for any integers $a,b\neq 0$ and any fixed interval I on the unit circle with positive measure, there is a positive propotion of χ's such that

$$L(1/2,\chi^a)L(1/2,\chi^b)\neq 0$$

and the normalize Gauss sum of χ is contained in I.

References

[1] Fouvry, É., Kowalski, E., Michel, Ph., *Algebraic trace functions over the primes*, Duke Math. J., **163**, 2014, 9, 1683–1736.

[2] Fouvry, É., Kowalski, E., Michel, Ph., Sawin, W., *Bilinear forms with trace functions*, https://arxiv.org/abs/2511.09459.

[3] Katz, N. M., *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of Mathematics Studies, **116**,1988.

[4] Katz, N. M., *Exponential sums and differential equations*, Annals of Mathematics Studies, **124**, 1990.

[5] Katz, N. M., Tiep, P. H., *Exponential sums, hypergeometric sheaves and monodromy groups*, Annals of Mathematics Studies, **220**, 2025.

[6] Sawin, Will, Forey, Arthur, Fresán, Javier and Kowalski, Emmanuel *Quantitative sheaf theory*, J. Amer. Math. Soc., **36**, 2023, 3, 653–726.

[7] Xu, J., *Stratification for multiplicative character sums*, Int. Math. Res. Not. IMRN, 2020, **10**, 2881–2917.

Determining distributions of algebraic objects from their moments

Melanie Matchett Wood

This talk includes joint work with Weitong Wang, Yuan Liu, David Zureick-Brown, Will Sawin. There are many distributions of algebraic objects that arise in number theory and beyond.

(1) For a finite group G, as $K/\mathbb{Q}$ varies over Galois G-extensions, what is the distribution of Cl_K? (Finite abelian G-module)
(2) As E varies over some collection of elliptic curves $/\mathbb{Q}$, what is the distribution of $\mathrm{Sel}_{p^\infty}(E)$, with the Cassels-Tate pairing? ($\mathbb{Z}_p$-module with alternating pairing)
(3) For a finite group G, as $K/\mathbb{Q}$ varies over Galois G-extensions, what is the distribution of $\mathrm{Gal}(K^{un}/K)$? (Profinite group with outer G-action)
(4) As M varies over (symmetric) $n \times n$ matrices with i.i.d. entries in $\{0, 1\}$, what is the distribution of $\operatorname{cok} M = \mathbb{Z}^n/M\mathbb{Z}^n$? (Finite abelian group, (with symmetric pairing))
(5) As M varies over closed, orientable 3-manifolds, what is the distribution of $\hat{\pi}_1(M)$? (Profinite group)

In general, the conjectures for these distributions reflect the algebraic structures themselves that are being distributed.

Conjecture 1 (Cohen–Lenstra [CL84]). *For any odd order abelian group A, for a random real quadratic field K,*

$$\mathrm{Prob}(\mathrm{Cl}_K^{\mathrm{odd}} \simeq A) = \frac{\prod_{p\geq 3}\prod_{i\geq 2}(1-p^{-i})}{|A||\operatorname{Aut}(A)|}.$$

Conjecture 2 (Cohen–Lenstra–Martinet [CM90], see (Wang-W. [WW21])). *For an abelian G-module A with $A^G = 1$ and $(|A|, |G|)$, for a random totally real G-extension $K/\mathbb{Q}$,*

$$\mathrm{Prob}(\mathrm{Cl}_K^{|G|'} \simeq_G A) = \frac{c}{|A||\operatorname{Aut}_G(A)|}.$$

Conjecture 3 (Delaunay [Del07], Bhargava–Kane–Lenstra–Poonen–Rains [BKLPR15]). *For a finite $\mathbb{Z}_p$-module A with a perfect alternating pairing $\langle , \rangle$, as E ranges over a natural family of rank 1 elliptic curves $\mathbb{Q}$,*

$$\mathrm{Prob}((\text{Ш}_E[p^\infty]; \langle , \rangle_{\mathrm{CT}}) \simeq (A; \langle , \rangle)) = \frac{c'}{|\operatorname{Aut}(A; \langle , \rangle)|}.$$

In particular, adding $\langle , \rangle$ to the isomorphism class does not add additional data!

$$\mathrm{Prob}(\text{Ш}_E[p^\infty] \simeq A) = \frac{c}{|\operatorname{Aut}(A; \langle , \rangle)|}$$

The entirety of the structure is not always obvious. If $K/\mathbb{Q}$ is a non-Galois quartic field, with Galois closure of Galois group D_4, $\operatorname{Aut}(K/\mathbb{Q}) = C_2$, so Cl_K is a C_2-module. More surprisingly, if $K/\mathbb{Q}$ is a degree 10 field, with Galois closure of Galois group A_5, $\operatorname{Aut}(K/\mathbb{Q}) = 1$, but $\mathrm{Cl}_K^{|A_5|'}$ is a C_2-module. (See W.-Wang [WW21] where it is shown that the heuristics reflect this.) For $K/\mathbb{Q}$ a G-extension, $\operatorname{Gal}(K^{un}/K)$ is the kernel of an exact sequence

$$1 \to \operatorname{Gal}(K^{un}/K) \to \operatorname{Gal}(K^{un}/\mathbb{Q}) \to G \to 1$$

If $\mu_n \subset K$, then $G = \operatorname{Gal}(K^{un}/K)$ comes with a fundamental class $s_K \in H_3(G, \mathbb{Z}/n)$ from Artin-Verdier duality. If M a symmetric matrix, $\operatorname{cok} M$ has a natural symmetric pairing.

In many cases, it is easier to solve the harder problem where you track more structure.

Theorem 1 (Liu, W., Zureick-Brown [LWZ24]). *Let G be a finite group, p a prime, and q a prime power with $p \nmid q(q-1)|G|$ and $(q, |G|) = 1$. Let $k = \mathbb{F}_q(t)$. For a random "totally real" G-extension K/k and a fixed finite $\mathbb{Z}_p[G]$-module A with $A^G = 1$*

$$\operatorname{Prob}(\mathrm{Cl}_K[p^\infty] \simeq_G A) \to \frac{c}{|A||\operatorname{Aut}_G(A)|} \text{ as } q \to \infty.$$

Also, analogous results for $\operatorname{Gal}(K^{un}/K)$.

Theorem 2 (Sawin, W., [SW25]). *As above but $(p, q-1) = n$, we determine distribution of* $(\mathrm{Cl}_K, s_K \in H_3(\mathrm{Cl}_K, \mathbb{Z}/n))$ *and* $(\operatorname{Gal}(K^{un}/K), s_K \in H_3(\operatorname{Gal}(K^{un}/K), \mathbb{Z}/n))$.

An important tool we have to determine the distribution of structures is through their moments. A random profinite group X has moments indexed by *finite groups*, instead of by natural numbers. The Gth moment is: $M_G(X) := \mathbb{E}[\# \operatorname{Sur}(X, G)]$.

Theorem 3 (Uniqueness of the moment problem for finite abelian groups, Wang-W. [WW21]). *Let X,Y be random finite abelian groups. If for each finite ab. group A,*

$$\mathbb{E}(\# \operatorname{Sur}(X, A)) = \mathbb{E}(\# \operatorname{Sur}(Y, A)) = O(|\wedge^2 A|),$$

then X and Y have the same distribution. ($|\wedge^2 \mathbb{F}_p^k| = p^{\frac{k^2-k}{2}}$)

Recently with Sawin, we have developed a theory for the moment problem for distributions of quite general algebraic structures.

Theorem 4 (Sawin-W. [SW22]). *For a random variable X valued in a* diamond category *(or its pro-completion), when the moments*

$$M_B := \mathbb{E}[\# \operatorname{Epi}(X, B)]$$

for all B aren't too large (according to a specific growth condition), they determine a unique distribution. We give an explicit condition for existence, and give (useful in practice) formulas for the distribution.

All of the above, and much much more, are diamond categories. In practice, generally Epi means surjections. We provide helper lemmas to let you check "aren't too large."

This theorem has already been applied in many different contexts to determine distributions of algebraic structures from their moments. Some examples include the following: Sawin-W. [SW24] π_1 of 3-manifolds; Smith [Smi25]: BSD implies Goldfeld's conjecture; Nguyen-W. [NW24]: cokernels of random (restricted coefficient) matrices, sandpile groups of Erős-Rényi random graphs; Yan [Yan24]: cokernels of random restricted coefficient matrices over a Dedekind domain; Cheong-Yu [CY23]: $\mathrm{cok}(P(M))$ for matrix M with independent restricted entries; Alberts [Alb23a]: random profinite groups to model absolute Galois groups (Law of Large Numbers on a category); Hodges [Hod24]: cokernels of symmetric (restricted coefficient) matrices with pairings; Huang-Nguyen-Van Peski [HNvP25]: cokernels of (restricted coefficient) matrix products; Shen [She25]: rational canonical form for (restricted coefficient) matrices over $\mathbb{F}_q$.

References

[Alb23a] Brandon Alberts. Counting Functions for Random Objects in a Category. (arXiv:2211.07129), March 2023.

[BKLPR15] Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra, Jr., Bjorn Poonen, and Eric Rains. Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves. *Cambridge Journal of Mathematics*, 3(3):275–321, 2015.

[CY23] Gilyoung Cheong and Myungjun Yu, *The distribution of the cokernel of a polynomial evaluated at a random integral matrix*, arXiv:2303.09125 [math.NT], 2023.

[CL84] Henri Cohen and Hendrik W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number Theory (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[CM90] Henri Cohen and Jacques Martinet. Étude heuristique des groupes de classes des corps de nombres. *Journal für die Reine und Angewandte Mathematik*, 404:39–76, 1990.

[Del07] C. Delaunay, Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics, in *Ranks of elliptic curves and random matrix theory*, 323–340, London Math. Soc. Lecture Note Ser., 341, Cambridge Univ. Press, Cambridge.

[Hod24] Eliot Hodges. The distribution of sandpile groups of random graphs with their pairings. *Transactions of the American Mathematical Society*, 377(12):8769–8815, December 2024.

[HNvP25] Yifeng Huang, Hoi H. Nguyen, and Roger Van Peski, *Cohen–Lenstra flag universality for random matrix products*, arXiv:2508.10127 [math.PR], 2025.

[LWZ24] Yuan Liu, Melanie Matchett Wood, and David Zureick-Brown. A predicted distribution for Galois groups of maximal unramified extensions. *Inventiones mathematicae*, April 2024.

[NW24] Hoi H. Nguyen and Melanie Matchett Wood. Local and global universality of random matrix cokernels. *Mathematische Annalen*, November 2024.

[She25] Jiahe Shen, *Universality of rational canonical form for random matrices over a finite field*, arXiv:2510.16225 [math.PR], 2025.

[Smi25] Alexander Smith, *The Birch and Swinnerton-Dyer conjecture implies Goldfeld's conjecture*, arXiv:2503.17619 [math.NT], 2025.

[SW22] Will Sawin and Melanie Matchett Wood. The moment problem for random objects in a category. *arXiv:2210.06279*, October 2022.

[SW24] Will Sawin and Melanie Matchett Wood. Finite quotients of 3-manifold groups. *Inventiones mathematicae*, April 2024.

[SW25] Will Sawin and Melanie Matchett Wood. Distributions of unramified extensions of global fields. available at https://people.math.harvard.edu/ mmwood/Publications/.

[WW21] Weitong Wang and Melanie Matchett Wood. Moments and interpretations of the Cohen–Lenstra–Martinet heuristics. *Commentarii Mathematici Helvetici*, 96(2):339–387, June 2021.

[Yan24] Eric Yan. Universality for Cokernels of Dedekind Domain Valued Random Matrices. *Michigan Mathematical Journal*, -1(-1):1–14, January 2024.

Twists, rank growths, Mordell-Lang, and Selmer groups

Sun Woo Park

(joint work with Daniel Keliher)

[Background]: We fix an elliptic curve E over a global field K. Given a positive number X, let $\mathcal{F}(X)$ be a finite set of isomorphism classes of quadratic extensions over K defined as

$$\mathcal{F}(X) := \left\{ L := K(\sqrt{d})/K : d \text{ square-free, } \operatorname{Nm}(d) \leq X \right\}$$

for some predetermined choice of a norm function $\operatorname{Nm} : K \to \mathbb{R}_{\geq 0}$.

Let j be a fixed non-negative integer. What is the asymptotic limit of the probability that the algebraic rank of $K(\sqrt{d})$-rational points of E is different from that of K-rational points of E by j, as the upper bound on the norm of d grows arbitrarily large, i.e.

$$\lim_{X \to \infty} \frac{\#\{K(\sqrt{d}) \in \mathcal{F}(X) : \operatorname{rk}(E(K(\sqrt{d}))) - \operatorname{rk}(E(K)) = j\}}{\#\mathcal{F}(X)} = ?$$

We note that the above question is equivalent to the problem of computing the distribution of algebraic ranks of K-rational points of quadratic twist families $\{E_d\}_d$ of E over K. Goldfeld's conjecture predicts that the above limiting probability is equal to $\frac{1}{2}$ when $j = 0$ or 1, and 0 when $j \geq 2$. There has been a wealth of significant progress towards the proof of Goldfeld's conjecture. A recent series of seminal groundbreaking works show that the validity of the Birch and Swinnerton-Dyer conjecture for quadratic twist families of elliptic curves implies Goldfeld's conjecture. The case when K is a number field is studied in a series of seminal works by Alex Smith [2, 3], and the case when K is a global function field is covered in the work by Jordan Ellenberg and Aaron Landesman [4], and the subsequent work by Aaron Landesman and Ishan Levy [5].

All of these works crucially use what is called the "Selmer group" of an elliptic curve over a global field K. Given a prime number p, the p-Selmer group of E

over K is defined as

$$\mathrm{Sel}_p(E/K) := \mathrm{Ker}\left(H^1(K, E[p]) \to \prod_{v \text{ place of } K} H^1(K_v, E)[p] \right).$$

The above construction can be generalized to any endomorphism of E defined over K. For the family of quadratic twists of E and $p = 2$, the elements of $\mathrm{Sel}_2(E_d/K)$ can be described more explicitly: they parametrize bi-quadratic extensions over the field $K(E[2])$ with certain ramification conditions at places $v \mid 2d\Delta_E\infty$, and unramified elsewhere. As this characterization suggests, $\mathrm{Sel}_p(E_d/K)$ is a finite set. Even better, its dimension as an $\mathbb{F}_p$-vector space gives an upper bound on the algebraic rank of $E_d(K)$. Therefore, it is a natural question to pursue what the distribution of $\mathrm{Sel}_p(E_d/K)$ is as $K(\sqrt{d})$ varies in $\mathcal{F}(X)$. The "Poonen-Rains heuristics" [6] predict the desired distribution to be the following:

$$\lim_{X\to\infty} \frac{\#\{K(\sqrt{d}) \in \mathcal{F}(X) : \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E_d(K)) = j\}}{\#\mathcal{F}(X)} = \prod_{k=0}^{\infty} \frac{1}{1+p^{-k}} \cdot \prod_{k=1}^{j} \frac{p}{p^k - 1}.$$

From now on, we will abbreviate the above conjectural probability as $PR(j)$ for each non-negative integer $j \geq 0$. All aforementioned seminal works focus on verifying the Poonen-Rains heuristics. Smith's work computes the distribution of 2^∞-Selmer groups, whereas Ellenberg, Landesman, and Levy's works compute the distribution of m-Selmer groups for all integers m coprime to $6 \cdot \mathrm{char}(K)$.

[Main Result]: In joint work with Daniel Keliher [1], we pursue the following two generalizations. We note that p is any odd prime, $f(x)$ is a degree 3 polynomial over K, and $\mathrm{rad}(I)$ is the radical of the ideal I.

(1) Prime cyclic extensions:
$\mathcal{F}(p, X) := \{L/K : \mathrm{Gal}(L/K) \cong \mathbb{Z}/p\mathbb{Z},\ \mathrm{Nm}^K_{\mathbb{Q}}(\mathrm{rad}(\Delta_{L/K})) \leq X\}.$

(2) Superelliptic curves:
$\mathcal{C}(p, X) := \{C_d/K : dy^p = f(x) : \mathrm{Nm}^K_{\mathbb{Q}}(\mathrm{rad}((d))) \leq X\}$

Assuming the extended Riemann hypothesis, we prove the following results.

(1) Suppose $\mathrm{Gal}(K(E[p])/K) \supset \mathrm{SL}_2(\mathbb{F}_p)$. Then

$$\liminf_{X\to\infty} \frac{\#\{L \in \mathcal{F}(p, X) : \mathrm{rk}(E(L)) - \mathrm{rk}(E(K)) \leq (p-1)\cdot j\}}{\#\mathcal{F}(p, X)} \geq \sum_{i=0}^{j} PR(i).$$

(2) Suppose $p \geq 5$, $K \supset \mathbb{Q}(\zeta_p)$, and $\mathrm{Gal}(f) \cong S_3$. Then there exists an explicit constant $B(p, K)$ depending only on the choice of p and K such that

$$\limsup_{X\to\infty} \frac{\sum_{C_d \in \mathcal{C}(p,X)} \#C_d(K)}{\#\mathcal{C}(p, X)} \leq B(p, K).$$

[Idea of Proof]: The proof of these results revolves around generalizing the work by Klagsbrun-Mazur-Rubin [7], which computes the distribution of Selmer groups using a different technique from [2, 3, 4, 5]. They construct a random walk governing the distribution of Selmer groups using the effective Chebotarev density theorem. As an example, suppose one has an elliptic curve $E : y^2 = x^3 + x - 1$ over $K = \mathbb{Q}$. The table below shows the distribution of $S_2(E_p) := \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_p/\mathbb{Q})$, where p ranges over the set of primes between 3 and 500000 and not equal to 31.

# roots $/\mathbb{F}_p$	$S_2(E_p) = 0$	$S_2(E_p) = 1$	$S_2(E_p) = 2$	$S_2(E_p) = 3$	$S_2(E_p) \geq 4$
0	25.04	74.96	0	0	0
1	37.41	25.01	37.58	0	0
3	12.56	65.95	12.49	9.00	0

The values inside the table correspond to conditional probabilities (in percentages) that $S_2(E_p) = k$ for some integer k, where p varies over a subset of primes such that $x^3 + x - 1$ has 3, 1, or no roots over $\mathbb{F}_p$. The distribution of $S_2(E_p)$ obtained from twisting E by a prime p can be modeled by, up to an error term determined by effective Chebotarev density theorem, a weighted sum of random walks

$$\mathbf{M} := \frac{1}{3} \cdot I + \frac{1}{2} \cdot M_2 + \frac{1}{6} \cdot M_2^2,$$

where I is the identity operator, and for each prime p the operator M_p is

$$M_p(r, s) := \begin{cases} \frac{1}{p^m} & \text{if } s = r + 1, \\ 1 - \frac{1}{p^m} & \text{if } s = r - 1, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, the average number of iterations of $\mathbf{M}$ is determined by the number of distinct prime factors of square-free numbers. By Erdös-Kac theorem, the distribution of $S_2(E_d)$, where the distinct prime factors of d grows at a certain rate respecting the effective Chebotarev density theorem, can be obtained by iterating $\mathbf{M}$ by roughly $\log \log |d|$ many times. The resulting distribution for $S_2(E_d) = j$ converges to $PR(j)$ for every non-negative integer j as $|d|$ grows arbitrarily large.

Likewise, we prove our main results by constructing a random walk $\mathbf{M}'$ obtained from taking a weighted sum of operators I, M_p, and M_p^2. Using $\mathbf{M}'$, we obtain that the desired distribution of Selmer groups of twist families of some auxiliary abelian varieties related to $\mathcal{F}(p, X)$ and $\mathcal{C}(p, X)$ conforms to a weighted version of Poonen-Rains heuristics. We achieve this by computing the asymptotic distribution resulting from applying $\mathbf{M}'$ arbitrarily many times. To reorder the non-canonically ordered family of fields from [7] by using $\mathrm{Nm}_{\mathbb{Q}}^{K}(\mathrm{rad}(\cdot))$, we combine the extended Riemann hypothesis with some results from sieve theory. The uniform boundedness on the average size of $C_d(K)$ can be achieved by combining the Poonen-Rains heuristics with uniform effective Mordell-Lang for curves, recently proven by Dimitrov-Gao-Habegger [8].

References

[1] Daniel Keliher and Sun Woo Park, *Distribution of Selmer ranks in prime cyclic extensions*, Preprint. 26 pages. (2025).

[2] Alexander Smith, *The distribution of ℓ^∞-Selmer groups in degree ℓ twist families I*, Journal of the American Mathematical Society. Vol. 39, Pages 1–72 (2026).

[3] Alexander Smith, *The distribution of ℓ^∞-Selmer groups in degree ℓ twist families I*, To appear at Journal of the American Mathematical Society. (2026).

[4] Jordan Ellenberg and Aaron Landesman, *Homological stability for generalized Hurwitz spaces and Selmer groups in quadratic twist families over function fields*, Preprint. 99 pages. (2023).

[5] Aaron Landesman and Ishan Levy, *The stable homology of Hurwitz modules and applications*, Preprint. 91 pages. (2025).

[6] Bjorn Poonen and Eric Rains, *Random maximal isotropic subspaces and Selmer groups*, Journal of the American Mathematical Society. Vol. 25, Pages 245–269 (2012).

[7] Zev Klagsbrun, Barry Mazur, and Karl Rubin, *A Markov model for Selmer ranks in families of twists*, Compositio Mathematica. Vol. 150, No. 7, Pages 1077–1106 (2014).

[8] Vesselin Dimitrov, Ziyang Gao, and Philipp Habegger, *Uniformity in Mordell-Lang for curves*, Annals of Mathematics. Vol. 194, No. 1, Pages 237–298 (2021).

Second moments for 2-Selmer structures on elliptic curves, and applications

Ashvin A. Swaminathan

(joint work with Manjul Bhargava, Wei Ho, Arul Shankar, Ari Shnidman)

The distribution of the rank of elliptic curves $E/\mathbb{Q}$ ordered by height remains a central open question in arithmetic statistics. The "Minimalist" Conjecture of Goldfeld and Katz-Sarnak predicts that 50% of elliptic curves have rank 0 and 50% have rank 1, with the average rank being 1/2. Since the rank $\operatorname{rk} E(\mathbb{Q})$ is difficult to compute directly, it has become of interest to study the p-Selmer groups $\operatorname{Sel}_p(E)$, which are more tractable and fit into the short exact sequence

$$0 \longrightarrow E(\mathbb{Q})/pE(\mathbb{Q}) \longrightarrow \operatorname{Sel}_p(E) \longrightarrow Ш_E[p] \longrightarrow 0.$$

In particular, it follows that $\operatorname{rk} E(\mathbb{Q}) \leq \operatorname{rk} \operatorname{Sel}_p(E)$, so it has become of interest to understand the distribution of p-Selmer ranks of elliptic curves. Poonen and Rains [5] developed a complete heuristic model for these Selmer groups, predicting the exact distribution of $\operatorname{rk} \operatorname{Sel}_p(E)$ for every prime p.

Very few cases of the Poonen–Rains heuristics hae been verified. The foundational work of Bhargava and Shankar [1, 2, 3] established the first moments for $p = 2, 3, 5$, finding that $\operatorname{Avg} \#\operatorname{Sel}_2(E) = 3$, $\operatorname{Avg} \#\operatorname{Sel}_3(E) = 4$, and $\operatorname{Avg} \#\operatorname{Sel}_5(E) = 6$. While these results imply that the average rank of elliptic curves is bounded, they do not rule out pathologies where a zero-density family of curves contributes nontrivially to the average. To control the variance, one requires information about the second moment. In 2021, Bhargava, Shankar, and the author [4] proved that for the family of all elliptic curves, $10 \leq \operatorname{Avg} \#\operatorname{Sel}_2(E)^2 \leq 15$. In particular, it follows from the upper bound that no zero-density subfamily contributes to the average size of $\operatorname{Sel}_2(E)$.

Our first contribution is to generalize these results to 2-Selmer structures $S(E)$, which are collections of local conditions defining subgroups of $H^1(\mathbb{Q}, E[2])$. For a family of elliptic curves $\mathcal{E}$ defined by local conditions and a sub-soluble 2-Selmer structure S, we prove:

Theorem 1 (Bhargava–Shankar–S.) *When elliptic curves over $\mathbb{Q}$ are ordered by height, we have that*

$$\operatorname{Avg}\#\mathrm{Sel}_S(E)^2 \le 1 + 6M(2;\mathcal{E};S) + 8M(2;\mathcal{E};S)^2,$$

where $M(2;\mathcal{E};S)$ is a product of local mass formulas.

To go beyond the second moment, we study the joint distribution of 2-Selmer groups in "twist hypercubes." Let $\mathcal{S}$ be a finite set of primes, and let $\overline{\mathcal{S}}$ be the set of squarefree integers composed of primes in $\mathcal{S}$. We consider the family of twisted curves $\{E^d : d \in \overline{\mathcal{S}}\}$. This set forms a hypercube of dimension $n = \#\mathcal{S}$, where the elements $d \in \overline{\mathcal{S}}$ correspond to vertices of a unit hypercube with coordinates defined by the prime divisors of d.

The 2-Selmer groups of the curves in this hypercube are not independent; their relationships are governed by Poitou-Tate duality, which dictates how dimensions change under quadratic twisting. We demonstrate that the valid configurations of 2-Selmer dimensions on this hypercube correspond bijectively to simple graphs on n vertices. By aggregating the constraints imposed by Poitou-Tate duality for a fixed set $\mathcal{S}$ and applying Theorem 1 to control intersections of 2-Selmer groups of elliptic curves in the corresponding hypercube, we formulate an infinite-dimensional linear programming problem for the probability distribution of 2-Selmer ranks. Solving this program via column generation for sets $\mathcal{S}$ of size up to 6 yields the following result:

Theorem 2. (Bhargava–Ho–Shnidman–S.) *For every $r \in \{0,1,2,3,4\}$, the probability that an elliptic curve over $\mathbb{Q}$ has 2-Selmer rank r is positive.*

This result provides the first proven lower bounds for the proportion of elliptic curves with prescribed 2-Selmer rank. In future work, we aim to extend our methods to prove similar lower bounds for each $r \geq 4$, with the goal of confirming a key prediction of the Poonen–Rains heuristics that every nonnegative integer occurs as a 2-Selmer rank with positive probability.

References

[1] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **177** (2013), no. 1, 21–93.

[2] M. Bhargava and A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. (2) **181** (2015), no. 2, 587–621.

[3] M. Bhargava and A. Shankar, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, preprint, arXiv:1312.7859 (2013).

[4] M. Bhargava, A. Shankar, and A. Swaminathan, *The second moment of the size of the 2-Selmer group of elliptic curves*, preprint, arXiv:2110.09063 (2021).

[5] B. Poonen and E. Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269.

Counting minimally ramified extensions of function fields

Mark Shusterman
(joint work with Jordan Ellenberg)

1. Homological Stability

It is by now well understood that purely topological theorems about homological stability for moduli spaces can be used to prove theorems in arithmetic statistics over global function fields. In more recent works it has become clear that there is utility in proving homological stability theorems where instead of studying the homology of the space itself, one studies the homology of local systems on that space. The moduli spaces in question are often $K(\pi, 1)$, so this reduces to computing the homology of the discrete group π with some of its representations as coefficients.

For instance, $\mathrm{Conf}^n(\mathbb{C})$ - the configuration space of n unordered distinct points in the plane is a $K(B_n, 1)$ where B_n is the Artin braid group on n strands given by the presentation

$$B_n = \langle \sigma_1, ..., \sigma_{n-1} : \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } i > j+1,\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ for } i < n-1\rangle.$$

The representations of B_n whose homological stability we study are of the form $V^{\otimes n}$ for a braided vector space V. Namely we have an isomorphism of vector spaces $T\colon V \otimes V \to V \otimes V$ for which

$$(\mathrm{id}_V \otimes T) \circ (T \otimes \mathrm{id}_V) \circ (\mathrm{id}_V \otimes T) = (T \otimes \mathrm{id}_V) \circ (\mathrm{id}_V \otimes T) \circ (T \otimes \mathrm{id}_V)$$

as (linear) maps from $V \otimes V \otimes V$ to $V \otimes V \otimes V$, and for $1 \leq i \leq n-1$ the generator $\sigma_i \in B_n$ acts as

$$\mathrm{id}_{V^{\otimes(i-1)}} \otimes T_V \otimes \mathrm{id}_{V^{\otimes(n-i-1)}}$$

on the vector space $V^{\otimes n}$.

Consider for example the vector space W with basis v, w braided by

$$v \otimes v \mapsto v \otimes v, \qquad v \otimes w \mapsto w \otimes v, \qquad w \otimes v \mapsto v \otimes w, \qquad w \otimes w \mapsto -w \otimes w.$$

The representation of B_n on $W^{\otimes n}$ is inflated from S_n via the surjective group homomorphism $B_n \to S_n$ that sends σ_i to the transposition $(i \quad i+1)$ for $1 \leq i \leq n-1$. The irreducible constituents of this representation are the wedge powers of the standard representation of S_n, each appearing with multiplicity 2.

A homological stability theorem in this setting is the assertion that, for each nonnegative integer i, the group $H_i(B_n, V^{\otimes n})$ is independent of n once n is large enough relative to i. A special case of our vanishing of homology result is the following.

Theorem 1. *Suppose that there exists a nonnegative integer d such that $H_0(B_n, V^{\otimes n}) = 0$ for every $n > d$. Then $H_i(B_n, V^{\otimes n}) = 0$ for $n > (d+2)i + d$.*

We have an analog of this theorem for surface braid groups, and we wonder whether there is an analog for automorphism groups of free groups, or for mapping class groups of connected closed orientable surfaces.

2. Arithmetic Applications

Let G be a nontrivial finite group, let p be a prime number not dividing $|G|$, and let q be a power of p. Let $R \subseteq G$ be a conjugacy class that generates G. Such a conjugacy class exists if and only if the abelianization of G is cyclic. We assume moreover that $r^q \in R$ for every $r \in R$.

Fix a separable tame closure $\overline{\mathbb{F}_q(t)}$ of $\mathbb{F}_q(t)$, a place of it lying over each (finite) place of $\mathbb{F}_q(t)$, and a (topological) generator of the corresponding (tame) inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{F}_q(t)}/\mathbb{F}_q(t))$. Note that every Galois extension of $\mathbb{F}_q(t)$ with Galois group G is tamely ramified.

For a nonnegative integer n denote by $\mathcal{E}_q^R(G;n)$ the family of regular Galois extensions L of $\mathbb{F}_q(t)$ inside $\overline{\mathbb{F}_q(t)}$ that are split completely at ∞, and are equipped with an isomorphism $\varphi\colon \mathrm{Gal}(L/\mathbb{F}_q(t)) \to G$ such that the chosen generators of inertia subgroups in $\mathrm{Gal}(\overline{\mathbb{F}_q(t)}/\mathbb{F}_q(t))$ of (finite) places ramified in L are mapped to R under the composition of group homomorphisms

$$\mathrm{Gal}(\overline{\mathbb{F}_q(t)}/\mathbb{F}_q(t)) \longrightarrow \mathrm{Gal}(L/\mathbb{F}_q(t)) \xrightarrow{\varphi} G.$$

The space Conf^n descends to a finite-type scheme over $\mathrm{Spec}\,\mathbb{Z}$, whose $\mathbb{F}_q$-points are the monic squarefree degree n polynomials in $\mathbb{F}_q[t]$, and for various braided vector spaces V, the representation $V^{\otimes n}$ of B_n descends to an étale sheaf on (an open subset of) $\mathrm{Spec}\,\mathbb{Z}$. The Frobenius trace functions of some of these sheaves are of interest in arithmetic statistics and analytic number theory. An example is the vector space of formal linear combinations of elements of R with braiding given on basis elements by

$$T(x \otimes y) = y \otimes y^{-1}xy, \qquad x, y \in R.$$

The value of the corresponding trace function on a monic squarefree $g \in \mathbb{F}_q[t]$ captures the number of $L \in \mathcal{E}_q^R(G;n)$ for which the product of the monic irreducible polynomials in $\mathbb{F}_q[t]$ that ramify in L is g.

A series of recent breakthroughs by Landesman–Levy obtained homological stability for this braided vector space. They then used the Grothendieck–Lefschetz trace formula, Deligne's upper bound on the eigenvalues of Frobenius acting on compactly supported étale cohomology, comparison of étale cohomology in characteristic p with singular homology, and a crude upper bound on the dimensions of unstable homology arising from an understanding of the homotopy type of $\mathrm{Conf}^n(\mathbb{C})$ in order to obtain an asymptotic for $\#\mathcal{E}_q^R(G;n)$ as $n \to \infty$ with q sufficiently large depending on $|G|$, thus going way beyond what is known for the analogous problem over $\mathbb{Q}$ in place of $\mathbb{F}_q(t)$.

Nigel Boston and Nadya Markin asked about the existence and count of $L \in \mathcal{E}_q^R(G;n)$ that are ramified at a single (finite) place of $\mathbb{F}_q[t]$. They observed that such an extension can only exist if G is generated by a single conjugacy class, which in the tamely ranified case is the conjugacy class of a generator of an inertia subgroup because $\mathbb{F}_q(t)$ has no regular unramified extensions.

In analytic number theory, given an arithmetic function with an asymptotic estimate for its sum, one is often interested in asymptotics for the sum of this function over the prime numbers (or monic irreducible polynomials). In our case the value of the function on a (monic squarefree) polynomial $g \in \mathbb{F}_q[t]$ is the number of $L \in \mathcal{E}_q^R(G;n)$ for which the product of all the monic irreducible polynomials in $\mathbb{F}_q[t]$ that ramify in L is g.

Regardless of the basic method being employed to estimate the sum of an arithmetic function over the primes - be it a (sophisticated) sieve, an identity such as that of Vaughn, or a convolution identity involving the Möbius function, an estimate for the sum of the function over the multiples of a given integer (or polynomial) which is allowed to grow with the range of summation is usually available. In our case, such an estimate is not provided by the works of Landesman–Levy, yet we manage to obtain the desired asymptotic.

Theorem 2. *For q sufficiently large depending on $|G|$, as $n \to \infty$ we have*

$$\#\{L \in \mathcal{E}_q^R(G;n) : L \textit{ is ramified at a single place of } \mathbb{F}_q(t)\} \sim \frac{q}{(q-1)n} \#\mathcal{E}_q^R(G;n).$$

A version of the problem not involving counting, only existence of G-extensions, and allowing ramification at a small number of primes, has been considered over global fields for instance in works of Bary-Soroker, Boston, Entin, Fehm, Hoelscher, Jones, Kisilevsky, Markin, Neftin, Nomura, Plans, Roberts, Schlank, Sonn, Ullom, and Witt. An upper bound for the version of our problem over $\mathbb{Q}$ with $G = S_4$ has been obtained by Bhargava–Ghate, and a lower bound for $G = S_3$ (respectively, $G = S_4$) with at most 3 (respectively, 8) ramified primes has been obtained by Taniguchi–Thorne.

The key inputs in our proof of Theorem 2 are Theorem 1, and a representation stability result of Landesman–Levy which relies on, among many other things, a large monodromy theorem of the speaker used in the proof of a large finite field analog of Theorem 2.

Theorem 2 can be used to guide one in making a conjecture for the analogous problem over $\mathbb{Q}$.

Theorem 2 has implications towards refinements of the Cohen–Lenstra heuristics where one cares about the factorization of the discriminant of the function field whose class group is studied.

There are some applications of this circle of ideas that may be pursued in future works. One such application, following our work with Wanlin Li, is to show that the asymptotic proportion among quadratic Dirichlet L-functions over $\mathbb{F}_q[t]$ with irreducible conductor of those having a zero at the central point $s = 1/2$ (or at any other given point) is 0. Another potential application, following the works of Landesman–Levy and Ellenberg–Landesman, would be to the distribution of Selmer groups of prime quadratic twists of an abelian variety over a global function field, and as a standard consequence, a result toward the minimalist conjecture for the rank of the Mordell–Weil group in this family.

The value at a degree n monic squarefree $g \in \mathbb{F}_q[t]$ of the trace function of the sheaf on Conf^n associated to (the inflation to B_n of) a finite-dimensional representation ρ of S_n is the character of ρ applied to the (conjugacy class of the) permutation of the roots of g in $\overline{\mathbb{F}_q}$ obtained by raising to qth power. Since we are interested in the irreducibility of g, or equivalently in Frob_q acting as an n-cycle on the roots of g, we can restrict attention to the wedge powers of the standard representations of S_n because the indicator function of n-cycles lies in the span of their characters. We incorporate these wedge powers into our picture by recalling that they appear in the nth tensor power of a braided vector space.

It would also be interesting to extend our results to irreducible representations of S_n other than the wedge powers of the standard representation, and work of Himes–Miller–Wilson makes significant progress in this direction.

It is quite conceivable that future work will extend Theorem 2 to function fields of arbitrary smooth projective curves over $\mathbb{F}_q$, to arbitrary groups G, and to ramification at any given number of places.

2.1. **Random Profinite Groups.** The work of Boston–Ellenberg suggests, among other things, the following random model of profinite groups. For each positive integer n consider the average over all the degree n irreducible polynomials $P \in \mathbb{F}_q[t]$ of the Dirac measure at the (maximal pro-prime-to-q quotient of the) étale fundamental group of $\operatorname{Spec} \mathbb{F}_q[t, P^{-1}]$ - the affine line punctured at the roots of P. Boston–Ellenberg postulate that as $n \to \infty$ these (averaged) probability measures converge (weakly) to a probability measure on a suitable space of profinite groups. The assumption that P is irreducible (or at least, has a bounded number of irreducible factors) is crucial for if dispensed with, a limiting probability measure as $n \to \infty$ will not exist.

Arithmetic topology furnishes us with an analogous random model of (profinite) 3-manifold groups with boundary - one selects a random knot in the 3-sphere and takes the profinite completion of the fundamental group of the complement in the 3-sphere of the interior of a tubular neighborhood of the knot. The analogy becomes particularly close if the knot is chosen as the closure of a random braid in B_n that maps to an n-cycle in S_n, and then the limit as $n \to \infty$ is taken.

A work of Sawin–Wood determines such a limiting probability distribution for the Dunfield–Thurston model of a random closed 3-manifold, and their follow-up work studies measures on profinite groups (and other categories) much more generally, emphasizing the key role of the G-moment in studying such distributions. The G-moment is the expectation of the number of surjections from a random profinite group in our model onto (the given finite group) G. Theorem 2 makes progress towards the computation of the G-moment for the random model of profinite groups proposed by Boston–Ellenberg.

For more on the topic of random algebraic objects we refer to Melanie Wood's contribution to this volume.

Probabilistic Galois theory in function fields

Alexei Entin

(joint work with Lior Bary-Soroker, Eilidh McKemmie, Alexander Popov, Himanshu Sharma)

We survey some recent results and work in progress on probabilistic Galois theory in function fields. A prototypical problem in classical Galois theory considers a random polynomial

$$f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$$

with $a_i \in \{1, \ldots, H\}$ $(H \geq 2)$ chosen uniformly and independently at random and asks to estimate the probability that $G_f = \mathrm{Gal}(f/\mathbb{Q}) = S_n$. In the *large box regime* where n is fixed and $H \to \infty$ it was conjectured by Van der Waerden and recently proved by Bhargava [Bha25] that $\mathbb{P}(G_f = S_n) = 1 + O(H^{-1})$. In the *small box regime* where H is fixed and $n \to \infty$ it is conjectured that $\mathbb{P}(G_f = S_n) = 1 + o(1)$, but this folklore conjecture remains open for every $H \geq 2$. Bary-Soroker, Koukoulopoulos and Kozma [BSKK23] showed that $\mathbb{P}(G_f = S_n \text{ or } A_n) = 1 + o(1)$ for $H \geq 35$ and Breuillard and Varjú showed the same for all $H \geq 2$ conditional on the Extended Riemann Hypothesis. Showing that A_n occurs with probability $o(1)$ remains an elusive challenge.

In recent years function field analogs of the above problem have been studied by the author and several collaborators (L. Bary-Soroker, E. McKemmie, A. Popov and H. Sharma). The basic model considers a random polynomial

$$f = X^n + a_{n-1}(t)X^{n-1} + \ldots + a_1(t)X + a_0(t)$$

with $a_i \in \mathbb{F}_q[t]_{\leq d}$ (the set of polynomials of degree $\leq d$, where $d \geq 1$) chosen uniformly and independently at random. For $f \in \mathbb{F}_q[t][X]$ we denote $G_f = \mathrm{Gal}(f/\mathbb{F}_q(t))$ (undefined if f is not separable). The following function field analog of the small box conjecture has been obtained.

Theorem 1 (E., Popov [EP24, Ent25]). *In the small box regime (q, d fixed, $n \to \infty$) and assuming q odd we have* $\mathbb{P}(G_f = S_n) = 1 - q^{-d} + o(1)$.

Note that in the function field case $G_f \neq S_n$ with positive limit probability. This reflects a unique function field phenomenon stemming from the fact that there are many roots of unity of low degree over $\mathbb{F}_q(t)$, which is not the case over $\mathbb{Q}$. In particular we were able to overcome the challenge of ruling out A_n. We can also determine the other types of Galois groups occuring with positive limit probability, they are of the form $S_{n-k} \times$ cyclic.

In a joint work with L. Bary-Soroker and E. McKemmie we also studied random *additive polynomials* of the form

$$f = X^{q^n} + a_{n-1}X^{q^{n-1}} + \ldots + a_1(t)X^q + a_0(t)X,$$

with $a_i \in \mathbb{F}_q[t]_{\leq d}$ drawn at random as above. Here the set of roots of f forms an n-dimensional $\mathbb{F}_q$-vector space (if $a_0 \neq 0$) and a priori $G_f \leq \mathrm{GL}_n(q)$.

Theorem 2 (Bary-Soroker, E., McKemmie [BSEM24])**.** *In the small box regime (q, d fixed, $n \to \infty$) and assuming q odd we have*

$$\mathbb{P}(G_f \supset \mathrm{SL}_n(q)) = 1 - q^{-d} + o(1).$$

We can describe precisely the Galois groups that occur with positive limit probability (and compute these probabilities) and we also treat the large box ($d \to \infty$) and large base field ($q \to \infty$) regimes.

In a work in progress joint with H. Sharma, we have also studied the Galois representations attached to a random Drinfeld module of large rank. If f is a random additive polynomial as above, it defines an $\mathbb{F}_q[T]$-module structure on $\overline{\mathbb{F}_q(t)}$ by the action $T \cdot \alpha = f(\alpha)$. This is a *Drinfeld module* of rank n over $\mathbb{F}_q(t)$ and (assuming $a_0 \neq 0$ which we do henceforth) it has an associated T-adic Galois representation $\rho_{f,T} : \mathrm{Gal}(\mathbb{F}_q(t)^{\mathrm{sep}}/\mathbb{F}_q(t)) \to \mathrm{GL}_n(\mathbb{F}_q[[T]])$.

These random Galois representations have been recently studied in the large box regime (q, n fixed, $d \to \infty$) by Ray [Ray24] who showed that $\mathrm{Im}(\rho_{f,T}) = \mathrm{GL}_n(\mathbb{F}_q[[T]])$ with limit probability 1. This was extended by Zywina [Zyw25] to the full adelic Galois representation associated with D_f, but only for rank $n = 2$.

The author and H. Sharma studied the same problem in the small box regime (q, d fixed, $n \to \infty$), which is more challenging. Provisional on a careful verification of all details, we can establish the following

Theorem 3 (E., Sharma 2025+)**.** *In the small box regime (q, d fixed, $n \to \infty$) and assuming q odd we have $\mathbb{P}\left(\mathrm{Im}(\rho_{f,T}) \supset \mathrm{SL}_n(\mathbb{F}_q[[T]])\right) = 1 - q^{-d} + o(1)$.*

We are also trying to describe precisely all the image groups occurring with positive limit probability. This is work in progress and a preprint should become available in the coming months.

References

[Bha25] M. Bhargava, Galois groups of random integer polynomials and van der Waerden's conjecture, Ann. of Math. (2) **201** (2025), no. 2, 339–377.

[BSEM24] L. Bary-Soroker, A. Entin and E. McKemmie, Galois groups of random additive polynomials, Trans. Amer. Math. Soc. **377** (2024), no. 3, 2231–2259.

[BSKK23] L. Bary-Soroker, D. Koukoulopoulos and G. Kozma, Irreducibility of random polynomials: general measures, Invent. Math. **233** (2023), no. 3, 1041–1120.

[Ent25] A. Entin, Galois groups of random polynomials over the rational function field, J. Lond. Math. Soc. (2) **111** (2025), no. 1, Paper No. e70061, 23 pp.

[EP24] A. Entin and A. Popov, Probabilistic Galois theory in function fields, Finite Fields Appl. **98** (2024), Paper No. 102466, 27 pp.

[Ray24] A. Ray. Galois representations are surjective for almost all Drinfeld modules. arXiv:2407.14264 [math.NT], 2024.

[Zyw25] D. Zywina. Drinfeld modules with maximal Galois action. arXiv: 2502.01030v1 [math.NT], 2025.

Divisor sums along binary forms

Mayank Pandey
(joint work with Wing Hong Leung)

We show the following pair of results.

Theorem 1. *There exist $c_1, \delta > 0, c_0$ such that*

$$\sum_{m,n<X} d(m^4+n^4) = X^2(c_1 \log X + c_0) + O(X^{2-\delta}). \tag{1}$$

Theorem 2. *There exist $c_2, \delta > 0, c_1, c_0$ such that*

$$\sum_{m,n<X} d_3(x^3+2y^3) = X^2(c_2 \log^2 X + c_1 \log X + c_0) + O(X^{2-\delta}). \tag{2}$$

In principle, our methods should apply to sums over general irreducible binary quartic and cubic forms in the case of Theorems 1 and 2, respectively, as well as with d and d_3 replaced by the Fourier coefficients of any GL_2 or GL_3 automorphic form, respectively.

Asymptotics for these were obtained by Daniel [Dan99] with remainder terms of size $O(X^2/(\log X)^{1-o(1)})$, exploiting the fact that values of binary quartic and cubic forms up to X have level of distribution $1/2$ and $2/3$ respectively, putting the two theorems right at the limit of the hyperbola method. To make this more concrete, we will discuss the case of Theorem 1 in more depth. Opening up the divisor function yields that

$$\sum_{m,n<X} d(m^4+n^4) \approx 2 \sum_{d \ll X^2} \sum_{m,n<X d|m^4+n^4} 1. \tag{3}$$

One can hope to estimate the inner sum accurately as long as $d \ll X^2/(\log X)^C$ for some $C > 0$ in the sense that one can hope for nontrivial bounds for

$$\sum_{d \ll X^2/(\log X)^C} \left| \sum_{m,n<X d|m^4+n^4} 1 - c\rho(d)\frac{X^2}{d} \right|, \tag{4}$$

and this is what Daniel shows with the geometry of numbers, using ideas due to Greaves. The case of $X^2/(\log X)^C \ll d \ll X^2$ may then be discarded at the cost of a remainder of size $X^2/(\log X)^{1-o(1)}$, and smaller remainders are not possible without exploiting the cancellation in the sum (4) without absolute values, for the inner sum on average has $O(1)$ terms when $d \sim X^2$.

It is this outer sum we are able to exploit to obtain a power saving. Key to our work is the observation that m^4+n^4 is a norm form in $K = \mathbb{Q}(\zeta_8)$, and therefore, by unique factorization, we may interpret the sum as one over values in $\mathcal{O}_K$ with ζ_8^2 and ζ_8^3 coefficients equal to 0. We detect that this pair of values is equal to 0 using a perturbation of a two-dimensional δ-symbol due to Li, Rydin-Myerson, and Vishe [LMV24].

As it happens, after two applications of Poisson summation (over $\mathcal{O}_K$) following the δ-method, Theorem 1 reduces to a subconvex estimate for cubic Dedekind zeta functions in the level aspect.

References

[Dan99] Stephan Daniel. On the divisor-sum problem for binary forms. *J. Reine Angew. Math.*, 507:107–129, 1999.

[LMV24] Junxian Li, Simon L. Rydin Myerson, and Pankaj Vishe. A two-dimensional delta symbol method and its application to pairs of quadratic forms. 11 2024. arXiv:2411.11355.

Upper bounds for number fields with even Galois group

Rainer Dietmann

(joint work with Sam Chow)

By the Hermite-Minkowski theorem, there are only finitely many number fields of given discriminant. Hence $F_n(X)$, the number of number fields $K \mid \mathbb{Q}$ of degree n and discriminant $|\Delta_K| \leq X$, is finite. Schmidt [6] famously obtained the upper bound $F_n(X) \ll_n X^{\sigma_n}$, where $\sigma_n = \frac{n+2}{4}$, which has been substantially improved for $n \geq 159$ in recent years. One can also study the related problem where in addition the Galois group is prescribed: For a positive integer n and a transitive subgroup $G < S_n$, let $F_n(X;G)$ be the number of number fields $K \mid \mathbb{Q}$ with discriminant $|\Delta_K| \leq X$ and $\mathrm{Gal}(\hat{K} \mid \mathbb{Q}) = G$, where $\hat{K}$ denotes the Galois closure of K over $\mathbb{Q}$ (of course trivially $F_n(X;G) \leq F_n(X)$). A conjecture of Malle predicts the order of magnitude of $F_n(X;G)$, but so far has only been proved for certain families of groups and in some special cases. Upper bounds on $F_n(X;G)$ have been established subsequently by several authors, including Bhargava's [2] result

$$F_n(X;G) \ll_{n,\varepsilon} X^{\sigma_n - 1 + \mathrm{ind}(G)^{-1} + \varepsilon}, \tag{1}$$

where $n - \mathrm{ind}(g)$ is the number of orbits of g on $\{1, 2, \ldots, n\}$, and $\mathrm{ind}(G) = \min\{\mathrm{ind}(g) : 1 \neq g \in G\}$. We recently [4] obtained the following new bound on $F_n(X;G)$ for even groups G, which improves on the best known bounds in a few cases.

Theorem 1. *Assume that $n \geq 6$ with*

$$n \notin \bigcup_{m \text{ odd}} \{m^2, m^2+1\}. \tag{2}$$

Further suppose that G is a proper transitive subgroup of A_n, and put $d = [S_n : G]$. Then

$$F_n(X;G) \ll_{n,\varepsilon} X^{E+\varepsilon},$$

where

$$E = E(G) = \sigma_n - 1 - \frac{1}{2n-2} + \sqrt{\frac{n}{4(n-1)d}} + \frac{n}{4n-4}.$$

This bound is stronger than (1) for the groups 6T12, 7T5, 8T48 in degrees 6,7,8, respectively (but the bound for 6T12 is superseded by an earlier quintic result, see [1]) and for 7T5 and 8T48 appears to be the best currently known.

Our proof builds on the aforementioned work of Schmidt and uses Galois resolvents to detect the property of the Galois group being a given (even) group G. This reduces the problem to bound above the number of solutions of a certain

Diophantine equation. To this end a version of the determinant method due to Salberger is used (see for example Lemma 1 in [3]). In one harder case the property that G is even is used in addition to exploit the discriminant being a square. At this point non-existence of certain lines on the discriminant variety needs to be established, using results from [5] and the assumption (2).

References

[1] B. Alberts, R. J. Lemke Oliver, J. Wang and M. M. Wood, *Inductive methods for counting number fields*, arXiv:2501.18574.

[2] M. Bhargava, Galois groups of random integer polynomials and van der Waerden's conjecture, Ann. of Math. (2) **201** (2025), 339–377.

[3] T. D. Browning, *Power-free values of polynomials*, Arch. Math. **96** (2011), 139–150.

[4] S. Chow, R. Dietmann, *Enumerative Galois theory for number fields*, https://arxiv.org/pdf/2304.11991.

[5] R. Dietmann, *Probabilistic Galois theory*, Bull. Lond. Math. Soc. **45** (2013), 453–462.

[6] W. M. Schmidt, *Number fields of given degree and bounded discriminant*, Astérisque **228** (1995), 189–195.

Zeros of Poincaré series

Noam Kimmel

Let $f \in M_k$ be a non-zero modular form of weight k for the full modular group $\mathrm{SL}(2,\mathbb{Z})$. It is known that such a form has roughly $k/12$ zeros in the fundamental domain $\mathcal{F} = \mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}$. Aside from some potentially forced zeros at i and $\rho = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ coming from the value of k mod 12, the rest of these $k/12$ zeros can be placed arbitrarily in $\mathcal{F}$ as f varies in M_k.

However, it is an interesting problem to try and understand the location of the zeros for distinguished modular forms within M_k. The first result in this direction is due to F. K. C. Ranking and Swinnerton-Dyer [5] who show that the zeros of Eisenstein series in $\mathcal{F}$ always lie on the geodesic connecting i and ρ. Since then their result has been generalized to many other families of distinguished modular forms (e.g. [1, 2, 8]).

The main new results of this talk concern the asymptotic distribution of the zeros of another class of distinguished modular forms - the Poincaré series. Let $P_{k,m} \in M_k$ be the Poincaré series of weight k and index m for the full modular group. In this talk I will consider the asymptotic behavior of sequences $(P_{k,m})_{k\geq 1}$ where the weight k goes to infinity and the index m is a function of k. Specifically, I we will explore the asymptotic distribution of the zeros of such sequences.

The case where $m = o(k)$ was considered by Rankin [6], who generalized the method in [5] and showed that in this case almost all of the zeros of $P_{k,m}$ in $\mathcal{F}$ lie on the geodesic connecting i and ρ. In [3] we generalize this result - for any fixed $\alpha \geq 0$ and any sequence $(P_{k,m})_{k\geq 1}$ with $m = \alpha k + o(k)$ we give a description for the asymptotic behavior of $(P_{k,m})_{k\geq 1}$. This includes also a description for the asymptotic distribution of the zeros.

Examining these distributions for various α, one can notice that they become increasingly more intricate as α grows. This might lead one to conjecture that if m

grows faster than αk for all $\alpha > 0$, then the zeros of $(P_{k,m})_{k\geq 1}$ equidistribute in $\mathcal{F}$. It turns out that this is true. To show this we use a result of Rudnick [7], where he showed that equidistribution of the zeros follows from a stronger condition called mass equidistribution (or Holomorphic Quantum Unique Ergodicity). In [4] we show that a sequence $(P_{k,m})_{k\geq 1}$ with $m \gg \alpha k \ \forall \alpha > 0$ and $m \ll k^{3/2-\epsilon}$ satisfies this condition, thereby also proving the equidistribution of zeros in these cases.

While the condition $m \gg \alpha k \ \forall \alpha > 0$ is necessary, the condition $m \ll k^{3/2-\epsilon}$ seems to be a limitation of the proof. It is interesting to try and extend this range and show equidistribution for a larger range of m's.

References

[1] Heekyoung Hahn. On zeros of Eisenstein series for genus zero Fuchsian groups. Proc. Amer. Math. Soc., 135(8):2391–2401, 2007.

[2] Paul Jenkins and Kyle Pratt. Interlacing of zeros of weakly holomorphic modular forms. Proc. Amer. Math. Soc. Ser. B, 1:63–77, 2014.

[3] N. Kimmel, Asymptotic zeros of Poincaré series, Int. Math. Res. Not. IMRN **2024**, no. 21, 13808–13826.

[4] N. Kimmel, Mass equidistribution for Poincaré series of large index, Q. J. Math. **76** (2025), no. 1, 265–285.

[5] F. K. C. Rankin and H. P. F. Swinnerton-Dyer. On the zeros of Eisenstein series. Bull. London Math. Soc., 2:169–170, 1970.

[6] R. A. Rankin. The zeros of certain Poincar´e series. Compositio Math., 46(3):255–272, 1982.

[7] Ze´ev Rudnick. On the asymptotic distribution of zeros of modular forms. Int. Math. Res. Not., 2005(34):2059–2074, 2005.

[8] J.-W. M. van Ittersum and B. Ringeling, On the zeros of odd weight Eisenstein series, Mathematika **71** (2025), no. 1, Paper No. e70004, 27 pp.

Revisiting Van der Waerden's problem in degree 4

Vlad Matei

Given any integer polynomial $f \in \mathbb{Z}[X]$ one of the basic questions one can ask is whether is irreducible or not. This is in general a difficult problem; for example, even for $f(X) = X^n + X^{n-1} + \ldots + X - 1$ we do not know whether it is irreducible or not, although it is conjectured to be irreducible. We now turn to the study of this question in a family.

For any positive integer H, let $E_n(H)$ denote the number of monic integer polynomials $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ of degree n with $|a_i| \leq H$ for all i such that the Galois group G_f of f is not S_n. Hilbert's Irreducibility Theorem implies that $E_n(H) = o(H^n)$, i.e., 100% of monic polynomials of degree n are irreducible and have Galois group S_n.

In 1936, van der Waerden [24] made this statement more quantitative and proved that

$$E_n(H) = O\Big(H^{\,n - \frac{1}{6(n-2)\log\log H}}\Big). \tag{1}$$

In the same paper, he also suggested the tantalizing and lasting conjecture that $E_n(H) = O(H^{n-1})$ for all n (clearly $E_n(H) \gg H^{n-1}$ as can be seen by setting

$a_n = 0$); and moreover, if we restrict ourselves to irreducible polynomials f with $G_f \neq S_n$, say this count is $B_n(H)$, then we should have $B_n(H) = o(H^{n-1})$.

Successive improvements to van der Waerden's result (1) were obtained by:

Knobloch [18] (1956), who proved that

$$E_n(H) = O\Big(H^{\,n-\frac{1}{18n(n!)^3}}\Big)\,;$$

Gallagher [16] (1973), who proved using his large sieve that

$$E_n(H) = O\Big(H^{\,n-1/2+\varepsilon}\Big)\,; \tag{3}$$

Zywina [27] (2010), who refined this to $E_n(H) = O(H^{n-1/2})$ for large n; Dietmann [13] (2013), who proved using resolvent polynomials and the determinant method that $E_n(H) = O\Big(H^{\,n-2+\sqrt{2}}\Big)$; and Anderson, Gafni, Lemke Oliver, Lowry-Duda, Shakan, and Zhang [1] (2021) who proved that $E_n(H) = O(H^{n-\frac{2}{3}+\frac{2}{3n+3}+\epsilon})$. Bhargava [5] almost settled the conjecture by showing that $B_n(H) = O(H^{n-1})$; while Chow and Dietmann [10] offered a different proof, but excluded as Galois group the alternating group A_n and the degrees $7, 8$ and 10.

For $n \leq 4$, van der Waerden's conjectured optimal upper bound of $o(H^{n-1})$ was proven by Chow and Dietmann [9].

More generally, how often does each group occur as the Galois group of a polynomial of a fixed degree $n \geq 3$? For $G \leqslant S_n$, let us write $N_{G,n} = N_{G,n}(H)$ for the number of monic, integer polynomials, with coefficients bounded by H in absolute value, whose Galois group is conjugate to G.

The question of understanding the behavior of $N_{G,n}$ for individual G has been the subject of many works, including [[24], [12], [9], [10],[27], [21], [8], [25], [26], [2]].

The fact that the bound $N_{G,n} = O(H^{n-1})$ holds for intransitive groups G was already shown by van der Waerden [24], using the fact that polynomials having such Galois groups are exactly those that factor over $\mathbb{Q}$. Moreover, an exact asymptotic of the form

$$\sum_{G \subset S_n \text{ intransitive}} N_{n,G} = c_n H^{n-1} + O(H^{n-2})$$

for an explicit constant $c_n > 0$ was obtained by Chela [8].

The Galois group G_f of an irreducible polynomial f acts transitively on its roots, that is, it is a transitive subgroup of S_n. This greatly limits the number of possibilities for the conjugacy class of G_f.

Widmer [25] has given excellent bounds in the case of imprimitive Galois groups G, using the fact that polynomials having such Galois groups are exactly those that correspond to number fields having a nontrivial subfield; specifically, his results imply that if $G \subset S_n$ is transitive but imprimitive, then

$$\sum_{G \subset S_n \text{ transitive but imprimitive}} N_{n,G} = O(H^{n/2+2}).$$

Bhargava [5] and Chow and Dietmann [10] showed that we have uniform power saving bounds for all transitive $G \neq S_n, A_n$; for example, Bhargava showed that if $G \neq S_n, A_n$ and $n \geq 53$ then $N_{G,n} = O(H^{n-3.5})$.

Despite the progress made on the question, very few bounds are sharp. Unlike in the number field case where we have Malle's conjecture that predicts the expected size of the count of numbers fields ordered by discriminant and prescribed Galois group, for our quantity $N_{n,G}$ there are almost no conjectures about its expected size.

In an upcoming paper, we revisit the degree 4 case and improve conditionally on Chow and Dietmann's result for A_4. They showed in [9] that $H \ll N_{4,A_4} \ll H^{5/2+\frac{1}{\sqrt{6}}+\varepsilon}$ for any $\varepsilon > 0$.

Theorem 1 (2025$^+$). *We have that*

$$H \log H \ll N_{4,A_4} \ll H^{5/2+6c+\varepsilon}$$

where c is any number such that for any nonsingular elliptic curve $E : y^2 = X^3 + AX + B$ with $A, B \in \mathbb{Z}$ the number of its integral points $\#E(\mathbb{Z}) \ll \Delta^c$; here $\Delta = -16(4A^3 + 27B^2)$ is the discriminant of the elliptic curve.

Remark. *Conjecturally $c = \varepsilon$ for any $\varepsilon > 0$. The best bound currently in the literature is $c = 0.1117... + \varepsilon$, see* [6].

References

[1] T. C. Anderson, A. Gafni, R. J. L. Oliver, D. Lowry-Duda, G. Shakan, and R. Zhang, *Quantitative Hilbert irreducibility and almost prime values of polynomial discriminants*, Int. Math. Res. Not. **2023** (2023), no. 3, 2188–2214.

[2] L. Bary-Soroker, O. Ben-Porath and V.Matei, *Probabilistic Galois Theory: The square discriminant case*, Bull. London Math. Soc., **56** (2024), 2162–2177.

[3] L. Bary-Soroker, D. Koukoulopoulos, and G. Kozma, *Irreducibility of random polynomials: general measures*, Invent. Math. **223** (2023), 1041–1129.

[4] L. Bary-Soroker and G. Kozma, *Irreducible polynomials of bounded height*, Duke Math. J. **169** (2020), no. 4, 579–598.

[5] M. Bhargava, *Galois groups of random integer polynomials and van der Waerden's Conjecture*, Ann. of Math. (2) **201**, 339 - 377, March 2025.

[6] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman and Y. Zhao,*Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves*, J. Amer. Math. Soc. **33** (2020), 1087-1099.

[7] E. Breuillard and P. P. Varjú, *Irreducibility of random polynomials of large degree*, Extracta Math. **223** (2019), no. 2, 195–249.

[8] R. Chela, *Reducible polynomials*, J. Lond. Math. Soc. **1** (1963), no. 1, 183–188.

[9] S. Chow and R. Dietmann, *Enumerative Galois theory for cubics and quartics*, Adv. Math. **372** (2020), 37 pp.

[10] S. Chow and R. Dietmann, *Towards van der Waerden's conjecture*, Trans. Amer. Math. Soc. **376** (2023), no. 4, 2739–2785.

[11] S. D. Cohen, *The distribution of galois groups and Hilbert's irreducibility theorem*, Proc. Lond. Math. Soc. **43** (1981), no. 2, 227–250.

[12] R. Dietmann, *On the distribution of Galois groups*, Mathematika **58** (2012), No. 1,35–44.

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

[14] S. Eberhard, *The characteristic polynomial of a random matrix*, Combinatorica **2022**, no. 42, 491–527.

[15] A. Ferber, V. Jain, A. Sah, and M. Sawhney, *Random symmetric matrices: rank distribution and irreducibility of the characteristic polynomial*, Math. Proc. Cambridge Philos. Soc. **174** (2023), no. 2, 233–246.

[16] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Proc. Sympos. Pure Math. **XXIV** (1973), 91–101.

[17] D. Hilbert, *Ueber die Irreducibilität ganzer rationaler functionen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. **110** (1892), 104–129.

[18] H.-W. Knobloch, *Die Seltenheit der reduzierbaren Polynome*, Jahresber. Dtsch. Math. **59** (1956), no. 1, 12–19.

[19] G. Kuba, *On the distribution of reducible polynomials*, Math. Slovaca **59** (2009), no. 3, 349–356.

[20] A. Landsman, R. J. Lemke-Oliver, and F. Thorne, *Improved lower bounds for the number of fields with alternating Galois group*, Bull. Lond. Math. Soc. **53** (2021), no. 4, 1159–1173.

[21] R. J. L. Oliver and F. Thorne, *Upper bounds on polynomials with small Galois group*,Mathematika **66** (2020), No. 4, 1054–1059.

[22] K. Mahler, *On some inequalities for polynomials in several variables*, J. Lond. Math. Soc. **37** (1962), no. 1, 341–344.

[23] K. Mahler, *On two extremum properties of polynomials*, Illinois J. Math. **7** (1963), no. 4, 681–701.

[24] B. L. van der Waerden, *Die Seltenheit der reduzierbaren Gleichungen und der Gleichungen mit Affekt*, Monatshefte für Mathematik und Physik **43** (1936), no. 1, 133–147.

[25] Martin Widmer. On number fields with nontrivial subfields. *International Journal of Number Theory*, 7(03):695–720, 2011.

[26] S. Y. Xiao, *On monic abelian cubics*, Compos. Math. **158** (2022), no. 3, 550–567.

[27] D. Zywina, *Hilbert's irreducibility theorem and the larger sieve*, arXiv:1011.6465, 2010.

Diagonal sums and random matrix integrals

Brad Rodgers

(joint work with Ofir Gorodetsky)

Recall the conjecture of Keating and Snaith [8] for moments of the Riemann zeta-function: for positive integers k,

$$\frac{1}{T}\int_T^{2T} |\zeta(1/2+it)|^{2k}\,dt \sim a(k)g(k)(\log T)^{k^2} \quad \text{as } T\to\infty, \tag{1}$$

where the constants $a(k)$ and $g(k)$ are defined by

$$a(k) := \prod_p \Big(1-\frac{1}{p}\Big)^{k^2} \sum_{j\geq 0} \frac{d_k(p^j)^2}{p^j}, \quad \text{and} \quad g(k) := \lim_{N\to\infty} \frac{1}{N^{k^2}} \int_{U(N)} |\det(1-g)|^{2k}\,dg.$$

This conjecture seems out of reach by current methods. A problem which can be analyzed more successfully and which bears some structural similarity was considered by Conrey and Gamburd [3]. Define

$$\mathfrak{m}_k(X) := \lim_{T\to\infty} \frac{1}{T}\int_T^{2T} \Big|\sum_{n\leq X} \frac{1}{n^{1/2+it}}\Big|^{2k}\,dt.$$

Conrey and Gamburd showed that

$$\mathfrak{m}_k(X) \sim a(k)\gamma(k)(\log X)^{k^2}, \quad \text{as } X\to\infty,$$

for $a(k)$ as before and $\gamma(k) = \mathrm{vol}(\mathcal{P}_k)$ where $\mathcal{P}_k$ is the k^2-dimensional polytope consisting of matrices $(x_{ij}) \in \mathbb{R}_{\geq 0}^{k^2}$ with all row sums satisfying $\sum_j x_{ij} \leq 1$, and all column sums satisfying $\sum_i x_{ij} \leq 1$.

The purpose of this talk was (i) to explain how a simple factorization device of Vaughan and Wooley [10] and Granville and Soundararajan [5] can be used to better understand the appearance of this polytope through a point count, and (ii) to make the combinatorial observation that only a small modification of this point count coincides with the right hand side of (1).

The factorization device can be described as follows. Say that a $k \times k$ matrix $A = (a_{rs})$ with positive integer entries is a *GCD grid* if $\gcd(a_{rs}, a_{pq}) = 1$ whenever $p < r$ and $q > s$. We use the notation $A \in \mathrm{Mat}^*_{k\times k}(\mathbb{N})$ to describe such matrices.

Proposition 1: If $m_1, ..., n_k$ are positive integers such that $m_1 \cdots m_k = n_1 \cdots n_k$, then there is a unique $A \in \mathrm{Mat}^*_{k\times k}(\mathbb{N})$ such that the row and column products satisfy

$$\mathrm{row}_r^{\times}(A) = m_r, \quad \mathrm{col}_s^{\times}(A) = n_s, \quad \text{for all } r, s.$$

Conrey and Gamburd's first step in proving their result is to note that

$$\mathfrak{m}_k(X) = \sum_{\substack{m_1\cdots m_k = n_1 \cdots n_k \\ m_i, n_j \leq X}} \frac{1}{(m_1 \cdots m_k n_1 \cdots n_k)^{1/2}}.$$

One may analyze this sum via a multiple contour integral and this is the approach taken in [3]. Alternatively, the above factorization tells us that the above sum is

$$= \sum_{\substack{A \in \mathrm{Mat}^*_{k\times k}(\mathbb{N}) \\ \mathrm{row}_r^{\times}(A),\, \mathrm{col}_s^{\times}(A) \leq X}} \frac{1}{\prod a_{pq}},$$

where the product is over all entries in the matrix. Keeping track of the finite collection of coprimality relations and approximating a lattice count with an integral it follows almost immediately that this is asymptotic to $a(k)\gamma(k)(\log X)^{k^2}$, with the k^2-dimensional polytope already appearing (in exponentiated form) in the sum above.

We make the observation that a small modification of the sum above induces the random matrix integral in (1). Define an *SE-chain* within a matrix to be a path of indices which can be traversed using only south $(1, 0)$ or east $(0, 1)$ increments, and define the *multiplicative length* of a matrix of natural numbers to be

$$L^{\times}(A) = \max\Big\{ \prod_{i=1}^{\ell} a_{p_i q_i} : \text{the indices } p_1q_1,\, p_2q_2,\, ..., p_\ell q_\ell \text{ lie on a single SE-chain}\Big\},$$

with the maximum taken over all SE-chains (of any possible length ℓ). We prove the following result.

Theorem 1: For positive integers k,

$$\sum_{\substack{A \in \mathrm{Mat}^*_{k\times k}(\mathbb{N}) \\ L^\times(A) \le T}} \frac{1}{\prod a_{pq}} \sim a(k)g(k)(\log T)^{k^2}, \quad \text{as } T \to \infty.$$

Similar results corresponding to moments of L-functions in orthogonal and symplectic families can also be proved, with the analogous factorization device in each case involving matrices with some symmetry imposed. The proofs depend on results in random matrix theory due in various forms to Rains [9], Gorodetsky [4], and Baik and Rains [1].

In ongoing work, we also use the same combinatorial framework to study moments of Dirichlet polynomials, showing that a conjecture of Conrey-Farmer-Keating-Rubinstein-Snaith [2] for shifted moments of the Riemann zeta-function implies that for $T = X^c$ with $c > 1/2$,

$$\frac{1}{T}\int_T^{2T} \Big| \sum_{n \le X} \frac{1}{n^{1/2+it}} \Big|^{2k} dt \sim a(k)\beta_k(c)(\log X)^{k^2},$$

where $\beta_k(c)$ is the volume of the k^2 dimensional polytope consisting of matrices $A \in \mathrm{Mat}_{k\times k}(\mathbb{R}_{\ge 0})$ with row sums and column sums satisfying $\mathrm{row}^+_r(A), \mathrm{col}^+_s(A) \le 1$ and *additive* length (defined in the obvious way) satisfying $L^+(A) \le c$. This interpolates between the regime of the Conrey-Gamburd theorem (relevant for short Dirichlet polynomials in which $c > k$) and the regime of the Keating-Snaith conjecture (relevant when $c < 1$, as $\zeta(1/2 + it)$ can be approximated by a long Dirichlet polynomial). Similar results also exist in the case that the Dirichlet polynomial $\sum_{n\le X} 1/n^{1/2+it}$ is replaced by the flat sum $\sum_{n \le X} n^{-it}$ (results of this sort were proved for random multiplicative functions in [6, 7]).

References

[1] J. Baik and E. M. Rains, *Algebraic aspects of increasing subsequences*, Duke Math. J. **109** (2001), no. 1, 1–65.

[2] 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.

[3] B. Conrey and A. Gamburd, *Pseudomoments of the Riemann zeta-function and pseudomagic squares*, J. Number Theory **117** (2006), no. 2, 263–278.

[4] O. Gorodetsky, *Magic squares, the symmetric group and Möbius randomness*, Monatsh. Math. **204** (2024), no. 1, 27–46.

[5] A. Granville and K. Soundararajan, *Large character sums*, J. Amer. Math. Soc. **14** (2001), no. 2, 365–397.

[6] A. J. Harper, A. Nikeghbali, and M. Radziwiłł, *A note on Helson's conjecture on moments of random multiplicative functions*, in *Analytic number theory*, 145–169, Springer, Cham, 2015.

[7] W. P. Heap and S. Lindqvist, *Moments of random multiplicative functions and truncated characteristic polynomials*, Q. J. Math. **67** (2016), no. 4, 683–714.

[8] J. P. Keating and N. C. Snaith, *Random matrix theory and $\zeta(1/2+it)$*, Comm. Math. Phys. **214** (2000), no. 1, 57–89.

[9] E. M. Rains, *Increasing subsequences and the classical groups*, Electron. J. Combin. **5** (1998), Research Paper 12, 9 pp.

[10] R. C. Vaughan and T. D. Wooley, *On a certain nonary cubic form and related equations*, Duke Math. J. **80** (1995), no. 3, 669–735.

Distribution of central values of additive twists of GL_2 L-series

Sary Drappeau

(joint work with Sandro Bettin, Jungwon Lee)

The L-series refered to in the title are series of the shape

$$L(x) = \sum_{n\geq 1} \frac{a(n)\mathrm{e}^{2\pi inx}}{\sqrt{n}} \tag{1}$$

where $a(n)$ are the Fourier coefficients of an automorphic form ϕ with respect to a group $\Gamma \subset \mathrm{SL}(2,\mathbb{R})$, normalized so that $a(n) = n^{o(1)}$ on average. This series makes sense whenever x is a cusp for Γ (*e.g.* for $x \in \mathbb{Q}$ if Γ is a Hecke congruence group in $\mathrm{SL}(2,\mathbb{Z})$). These cusps admit a natural ordering by denominators, and we observe that the size of $L(x)$ tends to grow, somewhat chaotically, as the denominator of x grows. This raises the question of the asymptotic distribution of these values among cusps of denominators at most Q, as $Q \to \infty$.

For holomorphic forms of weight 2, the value $L(x)$ (viewed as a function of the form) coincides with the modular symbol $\{x, \infty\}$. Mazur-Rubin [4] conjectured a Gaussian distribution. This was shown, in the average sense described above, by Petridis-Risager [6], for holomorphic forms of weight 2; and later by Nordentoft [5] for all weights.

Using a completely different method, Lee-Sun [3] and Bettin-Drappeau [1] have established that a CLT holds for forms over $\mathrm{SL}(2,\mathbb{Z})$ [1] or a congruence subgroup [3]. This method, based on dynamical systems, did not require the holomorphicity or cuspidality of the form, which led to a proof of the CLT for Maaß forms over $\mathrm{SL}(2,\mathbb{Z})$ in [2]. However it relied on dynamical properties of the Gauss map.

The situation was therefore somewhat unconfortable regarding unneeded assumptions (holomorphicity, or link with $\mathrm{SL}(2,\mathbb{Z})$). This left open, for instance, the case Maaß cusp forms for groups other than $\mathrm{SL}(2,\mathbb{Z})$; or more prosaically the case

$$a(n) = r_2(n) = \{(a,b) \in \mathbb{N}, n = a^2 + b^2\}$$

of the function counting the representation of n as sums of two squares (this corresponds to a non-cuspidal form for $\Gamma_0(4)$).

I reported on the work in progress joint with Sandro Bettin and Jungwon Lee in which we lift the unneeded assumptions.

Theorem 1. *Assume Γ is a cofinite group with cusps, let ϕ be automorphic for Γ with integer weight k and eigenvalue λ_ϕ, and let $L(x)$ be defined by* (1)*. Assume that either ϕ is cuspidal, or else $\lambda_\phi \geq 1/4$. Then there exists $\beta \in \{0, 1, 3\}$ and a positive symmetric 2×2 matrix Σ for which the following holds.*

As $Q \to \infty$, the random variable

$$\frac{L(x)}{\sqrt{(\log Q)(\log\log Q)^{\beta}}}$$

where $x \in (0,1)$ is chosen at random among cusps of Γ of denominators $\leq Q$, converges to a centered complex Gaussian with covariance matrix Σ. We have

$$\beta = \begin{cases} 0 & (\phi \textit{ cuspidal}) \\ 1 & (\lambda_\phi > 1/4), \\ 3 & (\lambda_\phi = 1/4 \textit{ (*)}) \end{cases}$$

((*)Actually the third condition is slightly more technical, it depends on the growth of ϕ at cusps).

The matrix Σ is a multiple of the identity matrix in the first two cases, and also in the third case if we assume that $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \Gamma \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \Gamma$.

When ϕ is cuspidal, we have explicitely $\Sigma = \sigma_\phi I_2$, where

$$\sigma_\phi = \frac{\|\phi\|_2}{\mathrm{Vol}(\Gamma\backslash\mathbb{H})\Gamma(1 - s_\phi + \frac{k}{2})\Gamma(s_\phi + \frac{k}{2})}.$$

The proof builds on the strategy in [1, 3] and uses Zagier's quantum modularity property [7] for $L(x)$, established in the quantitative sense which we need in [2]: for all $\gamma \in \Gamma$, the map

$$h_\gamma(x) = L(\gamma x) - L(x)$$

initially defined on cusps (except ∞ and $\gamma^{-1}\infty$) Hölder regular, and we have some information on its growth. One of the main novel ingredients is a theorem of Baladi-Vallée type (which we do not state here) for Bowen-Series expansions of cusps. There the rôle of the Gauss map is played by the Bowen-Series map. Much of the effort goes into reducing the hypothesis of this theorem so that we have a hope to be able to apply in our case. The main point is that the maps h_γ, although regular, do not possess an explicit expression (which makes it non-trivial to analyze their joint (γ, x) dependence). For the same reason, it turned out challenging to actually compute the parameters of the CLT, since these arrive naturally expressed in terms of h_γ.

References

[1] S. Bettin and S. Drappeau. Limit laws for rational continued fractions and value distribution of quantum modular forms. *Proc. London Math. Soc.*, 125(6):1377–1425, 2022.

[2] S. Drappeau and A. C. Nordentoft. Central values of additive twists of Maaß forms *L*-functions. arXiv preprint, 2022.

[3] J. Lee and H.-S. Sun. Dynamics of continued fractions and distribution of modular symbols. to appear at J. Eur. Math. Soc.

[4] B. Mazur and K. Rubin. Arithmetic conjectures suggested by the statistical behavior of modular symbols. *Exp. Math.*, 32(4):657–672, 2023.

[5] A. C. Nordentoft. Central values of additive twists of cuspidal L-functions. *J. Reine Angew. Math.*, 2021(776):255–293, 2021.

[6] Y. N. Petridis and M. S. Risager. Arithmetic statistics of modular symbols. *Invent. Math.*, 212:997–1053, 2018.

[7] D. Zagier. Quantum modular forms. In *Quanta of maths*, volume 11 of *Clay Math. Proc.*, pages 659–675. Amer. Math. Soc., Providence, RI, 2010.

On the number of solutions of decomposable form inequalities

C. L. Stewart

Let $d > n \geq 2$ and $\mathbf{X}= (X_1, ..., X_n)$. Suppose that F is a non-zero decomposable form in n variables with integer coefficients and degree d. Let V_F denote the volume of the set

$$\{(x_1, ..., x_n) \in \mathbb{R}^n : |F(x_1, ..., x_n)| \leq 1\}.$$

(V_F may be infinite.) We may factor F as

$$F(\mathbf{X}) = C_0 F_1(\mathbf{X})^{l_1} ... F_k(\mathbf{X})^{l_k}, \tag{1}$$

where $|C_0|$ is the content of F and $F_1, ..., F_k$ are distinct irreducible polynomials with integer coefficients, content 1 and degrees $d_1, ..., d_k$ respectively and $l_1, ..., l_k$ are positive integers for which $d_1 l_1 + ... + d_k l_k = d$. Each polynomial $F_i(\mathbf{X})$ determines exactly one maximal rational subspace of $\mathbb{R}^n$, say A_i, for which $F_i(\mathbf{X}) = 0$. Put

$$d_F = \begin{cases} 0 & \text{if } A_i = \{\mathbf{0}\} \text{ for } \ i = 1, ..., k \\ \max\{l_{i_1} d_{i_1} + ... + l_{i_j} d_{i_j}\} & \text{otherwise,} \end{cases} \tag{2}$$

where the maximum is taken over those tuples $(i_1, ..., i_j)$ of distinct integers for which $A_{i_1} \cap ... \cap A_{i_j}$ is different from the zero vector or equivalently for which there is a non-zero integer point $(s_1, ..., s_n)$ for which $F_{i_m}(s_1, ..., s_n) = 0$ for $m = 1, ..., j$.

F is said to be of *essentially finite type* if V_F is finite, $V(\tilde{F})$ is finite whenever $\tilde{F}$ is F restricted to a rational subspace of $\mathbb{R}^n$ which is not a subspace of A_i for $i = 1, ..., k$ and

$$A_1 \cap ... \cap A_k = \{\mathbf{0}\}. \tag{3}$$

Let $N_F^*(m)$ denote the number of vectors $(a_1, ..., a_n)$ with integer coordinates for which

$$0 < |F(a_1, ..., a_n)| \leq m. \tag{4}$$

Let $F(\mathbf{X})$ be a non-zero decomposable form in n variables with integer coefficients and degree d with $d > n \geq 2$ and let m be a positive integer. If F is of essentially finite type then we are able to prove that

$$N_F^*(m) \ll_{n,d} m^{\frac{1}{d} + \frac{n-1}{d-d_F}}. \tag{5}$$

This result generalizes a result of Thunder [2]. A key ingredient in the proof is a quantitative version of Schmidt's Subspace Theorem due to Evertse [1].

References

[1] J.-H. Evertse, An improvement of the quantitative Subspace theorem, *Compositio Math.* **101** (1996), 225–311.

[2] J.L. Thunder, Decomposable form inequalities *Annals of Math.* **153** (2001), 767–804.

Bogomolov and Lehmer type bounds and rational points of small rank on algebraic varieties

Evelina Viada

Let V be an algebraic irreducible proper subvariety of a torus or of an abelian variety G defined over $\overline{\mathbb{Q}}$. A leading principle in diophantine geometry is to describe via arithmetic properties large subsets of V that are non-dense in V.

A landmark of this principle is the Mordell Conjecture, proven by Faltings [11]. It claims that a curve of genus at least 2 embedded in its Jacobian has a finite number of rational points. This beautiful result has fascinated many mathematicians, inspiring a number of articles. The proof of this theorem is not effective in the sense that we do not have an algorithm to determine such points. This is due to the fact that, in general, it is still unknown how to give an effective or an explicit bound for the height of such a set. This remains a difficult open problem, in the context of the so-called effective or explicit Mordell conjecture.

More in general, we say that $V \subset G$ is *a torsion variety* (resp. *a translate*) if it is a finite union of translates of algebraic subgroups of G by torsion points (resp. by points). Moreover a proper irreducible subvariety $V \subsetneq G$ is *weak-transverse* (resp. *transverse*) if it is not contained in any proper torsion variety (resp. any proper translate).

Theorem 1 (*Mordell-Lang Conjecture*, proven by Faltings [11, 12] and Vojta [20])**.** *Let Γ be a subgroup of G of finite rank. Suppose that $V \subset G$ is not a translate. Then, the set $V \cap \Gamma$ is not Zariski dense in V.*

This implies the general Mordell Conjecture via the Mordell-Weil Theorem, which asserts that the set of k-rational points of an abelian variety defined over a number field k is a finitely generated group. Thus, for a subvariety V of an abelian variety that is not a translate, the set of rational points $V(\mathbb{Q})$ of V is non dense in V.

The Torsion Anomalous Conjecture gives a general framework of which the Mordell-Lang and other conjectures become special cases. Probably, the first special case of this conjecture was addressed in 1965 by Schinzel [17], who asked when points of rank one are dense in a variety $V \subset \mathbb{G}_m^n$ of codimension 2. The rank of a point is the smallest dimension of an algebraic subgroup containing the point. In 1999, a central paper of Bombieri, Masser and Zannier [2] for transverse curves in $\mathbb{G}_m^n$ gave new life to the question. For the first time to our knowledge, they used a Lehmer type bound to prove the finiteness of points of rank $n-2$ on a transverse curve. Their work is effective, and it inspired a major research activity.

We say that an irreducible variety $Y \subset V$ is a *V-torsion anomalous* variety if

(i) Y is a component of $V \cap (B + \zeta)$ with $B + \zeta$ an irreducible torsion variety of G;

(ii) the dimension of Y is larger than expected, i.e. the codimensions satisfy

$$\operatorname{codim} Y < \operatorname{codim} V + \operatorname{codim} B.$$

We say that Y is *maximal* if it is not strictly contained in another V-torsion anomalous variety.

The Torsion Anomalous Conjecture (TAC) can then be formulated as follows.

Conjecture 1 (TAC). *An irreducible subvariety V of G contains only finitely many maximal V-torsion anomalous varieties.*

It is not difficult to see that the TAC implies the Mordell-Lang Conjecture. The case of hypersufaces reduces to the Manin-Mumford Conjecture. Unfortunately, the TAC is only proven for curves in abelian varieties, and for varieties of codimension 2 in $\mathbb{G}_m^n$ and E^N. However, some cases are proven in an effective way and this has consequences on the effective Mordell-Lang Conjecture. This is how we find the rational points of small rank on some varieties.

Some classical examples where one can find the rational points, are mainly given for curves of genus 2 or 3 and rely either on the method of Chabauty [5] and Coleman [8], or on the Manin-Demjanenko method [9, 15]. In 2019, with Checcoli and Veneziano [7], and in 2022 with Veneziano [19], we introduced an explicit method to find the rational or even k-rational points on families of transverse curves embedded in E^N where $E(k)$ has rank at most $N-1$. In work in progress, partially joint with A. Galateau and R. Pengo, we investigate a different approach that allows us to give a method to find the k rational points of a variety V transverse in E^N where $E(k)$ has rank 1. The method can be extended to abelian varieties of the kind A^N where A is a simple abelian variety and the dimension of V is small with respect to N. Also some other abelian varieties can be considered, however the complexity of the endomorphism ring and non-sharp results on heights in abelian variety, make the constants huge and therefore not suitable for examples. We hope to get examples of surfaces in E^3 where we can determine all the rational points.

Our method relies on different results in arithmetic geometry. We use a Bogomolov type bound by Galateau that we make functorial and explicit. This is an explicit version of a generalization of a conjecture by F. Bogomolov [1]. For a variety $V \subset G$, we define the essential minimum $\mu(V)$ as the infimum of the $\theta \in \mathbb{R}$ so that the set of points of V of height $\leq \theta$ is Zariski dense in V. Then we have

Theorem 2 (*Bogomolov Conjecture*, proven by Ulmo [18] and Zhang [22]). *A variety $V \subset G$ is non torsion if and only if its essential minimum $\mu(V)$ is strictly positive.*

We then use a Lehmer type bound recently proven by E. Gaudron and G. Rémond and we make it functorial. These are bounds that generalise to points in an abelian variety the Dobrowolski bound in the context of the so called Lehmer conjecture [14]. More precisely, in [10] Dobrowolski essentially proves that there exists a constant $c > 0$ such that for any algebraic number α which is not a root of unity, one has

$$h(\alpha) \geq \frac{c}{[\mathbb{Q}(\alpha):\mathbb{Q}]}\left(\frac{\log 3[\mathbb{Q}(\alpha):\mathbb{Q}]}{\log\log 3[\mathbb{Q}(\alpha):\mathbb{Q}]}\right)^{-3}.$$

Moreover we use the explicit version by Philippon of the arithmetic Bézout's theorem [16, Theorem 3], Zhang's inequality [21, Theorem 5.2] and sharp diophantine approximations, such as the Siegel Lemma of Bombieri and Vaaler [3, Theorem 12].

Unfortunately, this is not sufficient to prove new cases of the TAC, but only finiteness results on special V-torsion anomalous varieties.

Our method is somehow complementary to the Chabauty method for surfaces by Caro and Pastén [4]. If the ambient variety G is a simple abelian variety, there is no way to make our strategy work. Instead, having a simple abelian variety is an advantage in their method. More precisely, they assume that G is a simple abelian variety, of dimension 3 and that $G(\mathbb{Q})$ has rank one. Then they sharply bound the number of rational points of some surfaces $V \subseteq G$, and they give an example in which they can find all rational points. However, their method does not work in E^3 and further restrictions, comparable to the assumption that the maximal V-torsion varieties are all points, are needed when $G = A_2 \times E$.

References

[1] F. A. Bogomolov, *Points of finite order on an abelian variety*, Math. USSR-Izv. **17** (1981), no. 1, 55–72.

[2] E. Bombieri, D. W. Masser and U. M. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*, Internat. Math. Res. Notices **1999**, (1999) no. 20, 1119–1140.

[3] E. Bombieri and J. D. Vaaler, *On Siegel's lemma*, Invent. Math. **73** (1983), no. 1, 11–32.

[4] J. Caro and H. Pastén, *A Chabauty-Coleman bound for surfaces*, Invent. Math. **234** (2023), no. 3, 1197–1250.

[5] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885.

[6] S. Checcoli, F. Veneziano and E. Viada, *On torsion anomalous intersections*, Atti Accad. Naz. Lincei Rend. Lincei Mat. Appl. **25** (2014), no. 1, 1–36.

[7] S. Checcoli, F. Veneziano and E. Viada, *The explicit Mordell conjecture for families of curves*, Forum Math. Sigma **7** (2019), Paper No. e31, 62 pp.

[8] R. F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770.

[9] V. A. Dem'yanenko, *Rational points of a class of algebraic curves*, Am. Math. Soc., Transl., II. Ser. **66** (1968), 246-272.

[10] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), no. 4, 391–401.

[11] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

[12] G. Faltings, *The general case of S. Lang's conjecture*, in *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)*, 175–182, Perspect. Math., 15, Academic Press, San Diego, CA.

[13] A. Galateau, *Une minoration du minimum essentiel sur les variétés abéliennes*, Comment. Math. Helv. **85** (2010), no. 4, 775–812.

[14] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. (2) **34** (1933), no. 3, 461–479.

[15] Y. I. Manin, *The p-torsion of elliptic curves is uniformly bounded*, Math. USSR, Izv. **3** (1969), 433–438.

[16] P. Philippon, *Sur des hauteurs alternatives. III*, J. Math. Pures Appl. (9) **74** (1995), no. 4, 345–365.

[17] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. **11** (1965), 1–34.

[18] E. Ullmo, *Positivité et discrétion des points algébriques des courbes*, Ann. of Math. (2) **147** (1998), no. 1, 167–179.

[19] F. Veneziano and E. Viada, *Explicit height bounds for k-rational points on transverse curves in powers of elliptic curves*, Pacific J. Math. **315** (2021), no. 2, 477–503.

[20] P. Vojta, *Integral points on subvarieties of semiabelian varieties. I*, Invent. Math. **126** (1996), no. 1, 133–181.

[21] S.-W. Zhang, *Positive line bundles on arithmetic varieties*, J. Amer. Math. Soc. **8** (1995), no. 1, 187–221.

[22] S.-W. Zhang, *Equidistribution of small points on abelian varieties*, Ann. of Math. (2) **147** (1998), no. 1, 159–165.

Parametrizing Galois extensions and rational connectedness

Danny Neftin
(joint work with Danny Krashen)

The geometry of parametrizing spaces of G-Galois extensions over a number field K is a subject of major interest in arithmetic geometry. For a fixed group G, such parametrizing spaces X always exist, and are represented by versal G-torsors $Y \to X$, but their geometry and their sets of rational points $X(K)$ are far from understood.

We consider *R-equivalence* (a.k.a. rational connectedness) on such parametrizing spaces X for G-Galois extensions of K. The notion of R-equivalence has been studied for tori, for algebraic groups, and for G finite over large (a.k.a. ample) fields K, but little is known concerning these parameterizing spaces/versal torsors for G-Galois extensions of number fields.

We represent G-Galois extensions as morphisms in the set

$$H^1(K,G) = \mathrm{Hom}(\Gamma_K, G)/\sim,$$

where Γ_K is the absolute Galois group of K, and $\sim$ is equivalence by inner automorphisms of G. We then say $\alpha, \beta \in H^1(K,G)$ are *R-equivalent* over K if there exist $\gamma_1(t), \ldots, \gamma_r(t) \in H^1(K(t),G)$, $r \geq 1$ with specializations: $\gamma_1(0) = \alpha$, $\gamma_r(1) = \beta$, and $\gamma_i(1) = \gamma_{i+1}(0)$ for $i = 1, \ldots, r$. Note that a single $\gamma_i(t)$ corresponds to a G-Galois extension $E_i/K(t)$ whose specializations at $t = 0$ and 1 are the G-Galois extensions corresponding to $\gamma_i(0)$ and $\gamma_i(1)$, resp., so that $E_1, \ldots, E_r/K(t)$ is a sequence of G-Galois extensions connecting the G-Galois extensions corresponding to α and β. In case $r = 1$, we say that α and β are simply R-connected.

The notion of R-equivalence, (or in particular, simple R-connectedness) is closely related to the property G-$\mathbf{BB}^n_K$. We say that G-$\mathbf{BB}^n_K$ holds if every n classes in $H^1(K,G)$ are the specializations of some $\gamma(t) \in H^1(K(t),G)$. The property G-$\mathbf{BB}^2_K$ is equivalent to simple R-connectedness and was first raised by Harbater. Fields K and groups G for which G-BB^2_K does not occur were given in by Colliot–Thélène, namely, with K a 2-adic field and $G = C_8$ the cyclic group of order 8, or with $K = F((t))$ for the field F of invariants of a certain p-group G. However, little is known about R-equivalence and G-$\mathbf{BB}^n_K$ over number fields K in the absence of a generic polynomial for G.

For abelian groups G and $K = \mathbb{Q}$, the existence of a generic (resp. parametric) extension for odd (resp. 2-power) order G over $\mathbb{Q}$ implies that $H^1(\mathbb{Q}, G)$ has G-$\mathbf{BB}^2_K$ and in particular is *R-trivial*, that is, has one R-equivalence class. However, already for quadratic fields K and the cyclic group $G = C_{2^s}$, the number of R-equivalence classes has so far been unknown. For Dihedral groups $G = D_{2^s}$ of order 2^{s+1}, it is known that $H^1(K, D_{2^s})$, $s = 2, 3$, have G-$\mathbf{BB}^2_K$ since a generic extension exists. However, so far the R-triviality of $H^1(K, D_{2^s})$ has been unknown for all $s \geq 4$.

We consider the number $r = r(K, G) := H^1(K, G)/R$ of R-equivalence class on $H^1(K, G)$ for basic families of groups G when a generic extension does not exist or is unknown to exist. We show that this r is sometimes also the minimal number of extensions of a rational function field $F = K(t_1, \ldots, t_d)$, $d > 0$ required to parametrize all G-Galois extensions, allowing the parametrization of G-Galois extensions for groups G that lack a generic extension. More specifically, we consider the stronger notion of dense parametrizations: say $\gamma_1, \ldots, \gamma_r \in H^1(F, G)$ *densely parametrizes* $H^1(K, G)$ if every $\alpha \in H^1(K, G)$ is a specialization of some γ_i in every open subset of a model X for F.

Already when G is abelian, $r(K, G) > 1$ is possible. All such nontrivial examples come from cyclic 2-groups $G = C_{2^s}$ where r is given as follows. Let $\mu_n = \langle \zeta_n \rangle$ denote the n-th roots of unity, $\operatorname{char} K$ the characteristic of K, and $\operatorname{Br}(L/K)$ the relative Brauer group of L/K. We then have:

Theorem 1. *Let K be a field of $\operatorname{char} K \neq 2$, let $s \geq 3$ be an integer, and $E \subseteq K(\mu_{2^s})$ the subfield fixed by conjugation $\zeta_n \to \zeta_n^{-1}$. Then the number of R-equivalence classes $r = \#H^1(K, C_{2^s})/R$ is the cardinality of the quotient of $\operatorname{Br}(K(\mu_{2^s})/K)$ by $\operatorname{Br}(E/K) + \operatorname{Br}(K(\sqrt{-1})/K)$. Furthermore, this r is the minimal number of extensions of a rational function field $K(t_1, \ldots, t_d)$, $d \in \mathbb{N}$, needed to (densely) parametrize $H^1(K, C_{2^s})$.*

Note that explicit $r(K, C_{2^s})$ extensions parametrizing $H^1(K, C_{2^s})$ were already given by Schneps, and Theorem 1 shows this is the minimal number of such extensions. For $G = C_{2^s}$, the theorem shows that $H^1(K, G)$ has the following Beckmann–Black-type property: Every $\alpha_1, \ldots, \alpha_n \in H^1(K, G)$, $n \geq 2$ which are R-equivalent are the specialization of some $\alpha \in H^1(K(t), G)$. The theorem leads to the number of R-equivalence classes and paramaetrizations for general abelian groups.

Theorem 2. *Let K be a field. Suppose that a finite group H acts on a cyclic group C of odd order coprime to $\operatorname{char} K$. Then the number $\#H^1(K, C \rtimes H)/R$ of R-equivalence classes coincides with that on $H^1(K, H)$. If furthermore $H^1(K, H)$*

is densely parametrized by r extensions of a K-rational function field, then so does $H^1(K, C \rtimes H)$.

As H and hence $G = C \rtimes H$ may not have a generic extension, this provides further examples of dense parametrizations in the absence of a generic extension. Note that C may be replaced by an odd order abelian group as long as the action of H is semisimple. In the opposite scenario where C is a cyclic 2-group, the analysis of R-equivalence on $H^1(K, C \rtimes H)$ is much more difficult, and even its finiteness is unknown. Among these, we focus on the basic family of Dihedral groups $D_{2^s} = C_{2^s} \rtimes C_2$, $s \geq 4$:

Theorem 3. *Let $s \geq 2$ and K be a number field. Then $H^1(K, D_{2^s})$ is R-trivial.*

Our approach considers R-equivalence on A-torsors in $\mathrm{H}^1(K, A)$, for finite abelian K-groups A. Our first observation relates R-equivalence on $\mathrm{H}^1(K, A)$ to R-equivalence on algebraic tori, a theory developed by Colliot–Thélène–Sansuc. Our starting point is the observation that the finiteness of R-equivalence classes on tori over finitely generated fields K implies that on $\mathrm{H}^1(K, A)$, and furthermore provides a dense parametrization:

Observation 4. *Let K be a finitely generated field, and A a finite K-group of order prime to* $\operatorname{char} K$. *Then the number r of R-equivalence classes in* $\mathrm{H}^1(K, A)/R$ *is finite, and it is the minimal number of torsors over $K(t_1, \ldots, t_d)$ needed to densely parametrize* $\mathrm{H}^1(K, A)$*, for all sufficiently large*

Our work motivates the following open question:

Problem 5. *Let G be a finite solvable group and K a number field. Is $r := \mathrm{H}^1(K, G)/R$ finite? In particular, is finiteness preserved under split extensions with abelian kernel? In case $r < \infty$, are there r extensions of a K-rational function field that parametrize* $\mathrm{H}^1(K, G)$*?*

It would also be interesting to find the number of parameters needed to parametrize $\mathrm{H}^1(K, G)$. In fact there is no known finite group G, for which its known that more than 2 parameters are needed to parametrize $\mathrm{H}^1(K, G)$.

Applying stratification theorems to counting integral points on thin sets of type II

Katharine Woo

(joint work with D. Bonolis, E. Kowalski, L. B. Pierce)

Let $F(Y, X_1, \ldots, X_n)$ be an absolutely irreducible polynomial in Y^d that is monic in Y. Define the counting function:

$$N(F, B) = \#\{\mathbf{x} \in \mathbb{Z}^n : \|\mathbf{x}\|_\infty \leq B, \exists y \in \mathbb{Z}, F(y, \mathbf{x}) = 0\}.$$

In nomenclature of Serre [11], bounding $N(F, B)$ corresponds to counting integral points in an affine thin set of type II. It was achieved separately by Cohen [6] and

Serre [11] that $N(F,B) \ll_{F,\epsilon} B^{n-1/2+\epsilon}$. This bound is sharp; this can be seen via inspecting the counting function for $F(Y,X_1,...,X_n) = Y^2 - X_1 - X_2 - ... - X_n$.

In this talk, I will present new work with D. Bonolis and L. B. Pierce that gives a wide class of polynomials for which we can go beyond this bound.

Theorem 1 (Bonolis, Pierce, Woo [4]). *Fix $n \geq 2$. Let $H(\mathbf{X}) \in \mathbb{Z}[X_1,\dots,X_n]$ be an irreducible polynomial and define $F(Y,\mathbf{X}) = Y^d - H(\mathbf{X})$ for an integer $d \geq 2$. Suppose there is no $L \in GL_n(\mathbb{Q})$ such that $H(L(\mathbf{X})) \in \mathbb{Z}[(X_i)_{i\in I}]$ for a subset $I \subsetneq \{1,\dots,n\}$. Then there is an integer $e(n) \geq 1$ such that for all $B \geq 1$,*

$$N(F,B) \ll_{n,\deg F,\epsilon} \log(\|F\|+2)^{e(n)} B^{n-1+\frac{1}{n+1}+\epsilon},$$

for all $\epsilon > 0$.

Further, we define the notion of a n-genuine polynomials – one that truly depends on all of its variables. We say that $F(Y,\mathbf{X})$ is n-genuine if every defining polynomial G for $\mathbb{Q}(\mathbf{X})[Y]/(F(Y,\mathbf{X}))$ satisfies that $\deg_Y(G), \deg_{X_i}(G) \geq 1$ for each i. We say that $F(Y,\mathbf{X})$ is n-allowable if $F(Y,L(\mathbf{X}))$ is n-genuine for each linear transform $L \in \mathrm{GL}_n(\mathbb{Q})$. We prove similar upper bounds for n-allowable polynomials; these polynomials may be of separate interest (in future work, we use these notions of n-genuineness to repair a small hole in the work of Cohen [6]).

Theorem 2 (Bonolis, Pierce, Woo [4]). *Fix $n \geq 2$. Let $F \in \mathbb{Z}[Y,X_1,\dots,X_n]$ with $\deg_Y F \geq 2$ be a monic n-allowable polynomial in Y^d with $d \geq 2$. Then there exists an integer $h = h(n,\deg F) \geq 1$ such that for all $B \geq 1$,*

$$N(F,B) \ll_{n,\deg F,\epsilon} \|F\|^h B^{n-1+\frac{1}{n+1}+\epsilon},$$

for every $\epsilon > 0$. If $\deg_Y F \geq 2$ and the same hypotheses hold with $d = 1$, the same result holds, conditional on GRH.

Under a stronger notion of genuineness (called strongly n-allowable in [4]), we can establish the bound $N(F,B) \ll_{n,\deg F,\epsilon} \log(\|F\|+2)^{e(n)} B^{n-1+\frac{1}{n+1}+\epsilon}$. A key strength of the above results is that they require no nonsingularity condition on $F(Y,\mathbf{X})$. Additionally, the condition of being n-allowable (resp. strongly n-allowable) is generic in the space of polynomials of degree $\deg_{X_i} F \leq D_i$ with a fixed dimension of the singular locus.

A main input for our work is the stratification theorem for exponential sums, developed by Fouvry, Katz and Laumon in [7, 8, 10]. Motivated by making the dependency in Theorem 1 and Theorem 2 on $\|F\|$ explicit, Bonolis, Kowalski and I establish that these strata vary uniformly in families, both algebraically and analytically.

Theorem 3 (Bonolis, Kowalski, Woo [2]). *Let n and D be positive integers. Let $F \in \mathbb{Z}[Y,X_1,,...,X_n]$ be a polynomial of total degree $\leq D$ which is monic in Y. There exist positive integers N and C and a stratification $\mathcal{X} = (X_j)$ with*

$$\mathbb{A}^n_{\mathbb{Z}} \supset X_1 \supset \cdots \supset X_n,$$

such that X_i is a homogeneous subvariety of codimension $\geq i$ and such that for all primes p not dividing N and for all $\mathbf{h} \in X_i(\mathbb{F}_p) \setminus X_{i+1}(\mathbb{F}_p)$, the bound

$$\left| \sum_{F(y,\mathbf{x}) \in \mathbb{F}_p^n} e_p(\mathbf{h} \cdot \mathbf{x}) \right| \leq Cp^{\frac{n+i}{2}}$$

holds, and moreover, the data $(\mathcal{X}, N, C)$ satisfies the following bounds:

(1) $C \ll_{n,D} 1$*;*
(2) $N \ll_{n,d} 1$*;*
(3) $\deg(X_i) \ll_{n,D} 1$ *for all i;*
(4) *the number of irreducible components of X_i is $\ll_{n,D} 1$;*
(5) *$ht(\mathcal{X}) \ll_{n,D} ht_c(F)$, i.e. one can write X_j as the common zero set of polynomials $(G_{j,1}, ..., G_{j,k})$ in such a way that $ht_c(G_{j,s}) \ll_{n,D} ht_c(F)$ for every indexing pair (j, s).*

References

[1] D. Bonolis. *A polynomial sieve and sums of Deligne type.* Int. Math. Res. Not. IMRN, (2):1096–1137, 2021.

[2] D. Bonolis, E. Kowalski and K. Woo, *Stratification theorems for exponential sums in families*, arXiv:2506.18299.

[3] D. Bonolis and L. B. Pierce. *Application of a polynomial sieve: beyond separation of variables.* Algebra Number Theory, 18(8):1515–1556, 2024.

[4] D. Bonolis, L.B. Pierce and K. Woo, *Counting integral points in thin sets of type II: singularities, sieves, and stratification*, arXiv:2505.11226.

[5] T. Buggenhout, R. Cluckers, T. Santens and F. Vermeulen, *Serre's question on thin sets in projective space.* arxiv:2506.13471.

[6] S. D. Cohen. *The distribution of Galois groups and Hilbert's irreducibility theorem.* Proc. London Math. Soc. (3), 43(2):227–250, 1981

[7] É. Fouvry: *Consequences of a result of N. Katz and G. Laumon concerning trigonometric sums*, Israel J. Math. 120 (2000), 81–96.

[8] É. Fouvry and N. Katz: *A general stratification theorem for exponential sums, and applications*, Crelle 540 (2001), 115–166.

[9] D. R. Heath-Brown and L. B. Pierce. *Counting rational points on smooth cyclic covers.* J. Number Theory, 132(8):1741–1757, 2012

[10] N.M. Katz and G. Laumon: *Transformation de Fourier et majoration de sommes exponentielles*, Publ. Math. IHÉS 62 (1985); 145–202; Corrigendum 69 (1989), 233.

[11] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 3rd edition, 1997. Translated from the French and edited by M. Brown from notes by M. Waldschmidt.

Generic conic bundle surfaces satisfy the Hasse principle

Efthymios Sofos

(joint work with Christopher Frei)

Deciding whether a Diophantine equation has a solution is one of the main question in number theory. The Hasse principle is the most common approach, however, it is known to fail for surfaces [8]. A well-known conjecture of Colliot-Thélène [2] states that the counter-examples are explained by the Brauer–Manin obstruction for smooth, projective, geometrically integral and geometrically rationally connected varieties defined over a number field. This includes conic bundle surfaces. These arise as smooth projective models of surfaces defined in $\mathbb{A}^1_{\mathbb{Q}} \times \mathbb{P}^2_{\mathbb{Q}}$ by equations of the shape

$$P_1(t)x^2 + P_2(t)y^2 = P_3(t)z^2, \tag{1}$$

with polynomials $P_i \in \mathbb{Z}[t]$ whose product $P_1P_2P_3$ is non-constant and separable. They appear naturally in algebraic geometry. For example, cubic surfaces with a line defined over $\mathbb{Q}$ are the same as (1) with $\deg(P_1) = 3, \deg(P_2) = 1 = \deg(P_3)$. Del Pezzo surfaces of degree 2 containing a conic over $\mathbb{Q}$ are the same as (1) with $\deg(P_i) = 2$ for all i. The Hasse principle is not known in the latter case.

When $\sum_{i=1}^3 \deg(P_i) \leq 4$ the conjecture was proved by Colliot-Thélène–Sansuc–Swinnerton-Dyer [3, 4] and Colliot-Thélène [1]. When $\sum_{i=1}^3 \deg(P_i) = 6$ some cases were dealt with by Swinnerton-Dyer [9]. The Hasse principle for conic bundle surfaces is not known in other cases.

Fix arbitrary integers $d_1, d_2, d_3 \geq 0$. Let S be a subset of $\mathbf{P} = (P_1, P_2, P_3) \in (\mathbb{Z}[t])^3$ with $\deg(P_i) = d_i$ and let $h(\mathbf{P})$ be the maximum of the absolute values of the integer coefficients appearing in P_1, P_2 and P_3. If

$$\lim_{H\to\infty} \frac{\#\{\mathbf{P} \in (\mathbb{Z}[t])^3 : \deg(P_i) = d_i \forall i, h(\mathbf{P}) \leq H, \mathbf{P} \in S\}}{\#\{\mathbf{P} \in (\mathbb{Z}[t])^3 : \deg(P_i) = d_i \forall i, h(\mathbf{P}) \leq H\}} = 1$$

then we say that S has probability 1.

Theorem 1 (C. Frei–E. Sofos [5]). *Fix arbitrary integers $d_1, d_2 > 0, d_3 \geq 0$. The set of $\mathbf{P} \in (\mathbf{Z}[t])^3$ with $\deg(P_i) = d_i$ for all i such that* (1) *satisfies the Hasse principle has probability* 1.

In [5] we also prove the Hasse principle with probability 1 for conic bundle surfaces of the form

$$\Big(\prod_{j=1}^{k_1} P_{1j}(t)\Big)x^2 + \Big(\prod_{j=1}^{k_2} P_{2j}(t)\Big)y^2 = \Big(\prod_{i=1}^{k_3} P_{3j}(t)\Big)z^2, \tag{2}$$

where the P_{ij} have prefixed degrees and at least two of the k_i are strictly positive. Allowing reducible polynomials gives richer Brauer obstructions. Previous work in this direction had established the Hasse principle with positive probability [6].

The proof is based on the second moment method: for each $\mathbf{P} = (P_1, P_2, P_3)$ we write a sum $S_{\mathbf{P}}$ that essentially counts t for which (1) has a rational point. It then suffices to prove a non-trivial bound for

$$\sum_{\substack{\mathbf{P}\in(\mathbb{Z}[t])^3, h(\mathbf{P})\leq H \\ \deg(P_i)=d_i\forall i}} \Big(S_{\mathbf{P}} - \prod_{\substack{\ell \text{ prime} \\ \ell=2}}^{\infty} \sigma_\ell(\mathbf{P})\Big)^2,$$

where $\sigma_\ell(\mathbf{P})$ are appropriate non-negative ℓ-adic densities. The reason is that if (1) has a solution in $\mathbb{R}$ and in $\mathbb{Q}_\ell$ for each prime ℓ then $\prod_\ell \sigma_\ell(\mathbf{P})$ typically stays away from 0.

To bound the second moment one opens up the square and computes all three resulting terms. In the case of (2) this becomes more challenging, hence, we we make an unusual choice for $S_{\mathbf{P}}$, one that involves a modified Hilbert symbol. Specifically, for a prime $p \neq 2$ and for elements $a, b \in \mathbb{Q}_p \setminus \{0\}$ we let $(a,b)'_p = 0$ if both p-adic valuations of a, b are even and we otherwise let $(a,b)'_p$ be the usual Hilbert symbol in $\mathbb{Q}_p$. Then for positive integers a, b, both of which are 1 modulo 4, we define

$$\delta(a,b) = \prod_{\substack{\ell \text{ prime} \\ \ell=3}}^{\infty} (1 + (a,b)'_\ell).$$

If this expression is non-zero then $ax^2 + by^2 = z^2$ has a rational point by the Hasse principle. The function δ has a similar definition for all integers a, b. We then let

$$S_{\mathbf{P}} := \sum_{\substack{s,t \in \mathbb{Z}^2, \gcd(s,t)=1 \\ |s|,|t| \leq B^c}} \delta(P_1(s,t)P_3(s,t), P_2(s,t)P_3(s,t)),$$

where c is a positive constant that depends only on d_i. The advantage of the modified Hilbert symbol is that correlations and other averages of $S_{\mathbf{P}}$ vanish because

$$\int_{\mathbb{Z}_p^2} (a,b)'_p \mathrm{d}a\mathrm{d}b = 0, \text{ whereas } \int_{\mathbb{Z}_p^2} (a,b)_{\mathbb{Q}_p} \mathrm{d}a\mathrm{d}b = 1 - O\left(\frac{1}{p}\right).$$

Here the integral is with respect the normalised p-adic Haar measure μ_p such that $\mu_p(\mathbb{Z}_p) = 1$.

When a, b are square-free coprime integers, both 1 modulo 4, we can use Hilbert reciprocity to write $\delta(a,b) = \delta_1(a,b) + \delta_2(a,b)$, where

$$\delta_1(a,b) = (1 + (a,b)_{\mathbb{R}}) \sum_{\substack{k \text{ square-free} \\ k|ab, k\leq z}} \prod_{p|k} (a,b)'_p$$

$$\delta_2(a,b) = \sum_{\substack{k \text{ square-free} \\ k|ab, z<k<|ab|/z}} \prod_{p|k} (a,b)'_p$$

and $z = H^\gamma$ with γ a small positive constant depending only on d_i. The functions δ_1, δ_2 can be defined in a similar way for all integers a, b. Solubility at small primes is tracked by δ_1, whereas, δ_2 is a large sum of alternating terms, thus, it contributes only to the error term. To show the latter we prove a result for general functions $f : \mathbb{Z}^n \to \mathbb{C}$. This states that if f has average 0 on arithmetic progressions of small moduli then its average over random integer forms of fixed degree is also 0. For notational simplicity we state it for $n = 1$ and polynomials instead of forms.

Let τ denote the standard divisor function.

Theorem 2 (C. Frei–E. Sofos [5])**.** *Fix any $C > 0$ and any integer $d > 0$. Let $f : \mathbb{N} \to \mathbb{C}$ be an arbitrary function with $|f(m)| \leq \tau(m)^C$ for all m. Then there* *exists* $\kappa = \kappa(d, C) > 0$ *such that for any* x, H *with* $(\log H)^\kappa \le x \le H$ *we have*

$$\frac{1}{H^{d+1}} \sum_{\substack{P \in \mathbb{Z}[t], h(P) \le H \\ \deg(P) = d}} \left| \frac{1}{x} \sum_{n \le x} f(|P(n)|) \right|^2 \ll x^{6d} \frac{(\log H)^\kappa}{H^2} \max_{\substack{0 < q \le x^d \\ a \in \mathbb{Z}/q\mathbb{Z}}} \left| \sum_{\substack{n \le Hx^d \\ n \equiv a \bmod q}} f(n) \right|^2 ,$$

where the implied constant depends only on C *and* d*.*

The first steps of the proof follow the circle method approach of Skorobogatov–Sofos [6] regarding the von Mangoldt function. Their approach crucially rests on Vinogradov type estimates for the von Mangoldt function on the minor arcs, however, to cover general f it is essential to use a more flexible approach. This is achieved by replacing the Dirichlet kernel in [6] by the heat kernel. It allows us to use a transformation law for the Jacobi theta function to show that the minor arcs essentially make no contribution. The major arcs give rise to the max-term in the right-hand side of the bound in Theorem 2.

It would be interesting to prove the Hasse principle with probability 1 for quadric bundles of relative dimension 2 improving on the positive probability result of Skorobogatov–Sofos [7, Corollary 2.5].

References

[1] J.-L. Colliot-Thélène, *Surfaces rationnelles fibrées en coniques de degré* 4, Séminaire de Théorie des Nombres, Paris 1988–1989, Progr. Math., Birkhäuser Boston, Boston, MA **91** (1990), 43–55.

[2] ———, *Points rationnels sur les fibrations*, Higher dimensional varieties and rational points (Budapest, 2001),Bolyai Soc. Math. Stud., Springer, Berlin **12** (2003), 171–221.

[3] 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.

[4] ——— *Intersections of two quadrics and Châtelet surfaces. II*, J. reine angew. Math. **374** (1987), 72–168.

[5] C. Frei, E. Sofos *Random conic bundle surfaces satisfy the Hasse principle*, Preprint (2025), 1–61.

[6] A. N. Skorobogatov, E. Sofos *Schinzel hypothesis on average and rational points*, Invent. Math. **231** (2023), 673–739.

[7] ——— *Generic diagonal conic bundles revisited*, Q. J. Math. **75** (2024), 835–849.

[8] P. Swinnerton-Dyer, *Two special cubic surfaces*, Mathematika **9** (1962), 54–56.

[9] ———, *Rational points on some pencils of conics with 6 singular fibres*, Ann. Fac. Sci. Toulouse Math. (6), **8** (1999), 331–341.

Summary of open problem session

Collected by Noam Kimmel

1. Sam Chow

Fix $n \geq 3$ and denote

$$E_n(H) = \# \left\{ \begin{array}{l} f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in \mathbb{Z}[x] \\ \mathrm{Gal}(f) \neq S_n, \quad f\text{irreducible} \\ |a_j| \leq H \; \forall j \end{array} \right\}.$$

In 1936 van der Waerden conjectured the following [9]:

$$E_n(H) = o(H^{n-1}).$$

Remark. *A weak version of van der Waerden's conjecture was solved by Bhargava* [1]*, namely that $E_n(H) \ll_n H^{n-1}$, and that if one also excludes polynomials with Galois group equal to A_n then the number of remaining polynomials is $o(H^{n-1})$.*

2. Gady Kozma

Let G be a group and S be a non-reversible set of generators (reversible meaning that $s \in S \iff s^{-1} \in S$). Let $P \in \mathrm{Mat}_{G \times G}$ be the Cayley graph matrix associated with G and S:

$$P_{g,h} = \begin{cases} 1 & \exists s \in S : g = hs \\ 0 & \text{otherwise.} \end{cases}$$

The question is whether being orthogonally Jordanisable is common among such Cayley matrices P?

3. Lior Bary-Soroker

The motivation for the following problem came from the 𝕏-post [5] where the following matrix multiplication was considered:

$$\begin{pmatrix} 6 & 5 & 3 & 7 \\ 3 & 2 & 1 & 3 \\ 5 & 3 & 2 & 5 \\ 7 & 5 & 3 & 6 \end{pmatrix} \cdot \begin{pmatrix} 7 & 2 & 1 & 2 \\ 1 & 1 & 3 & 1 \\ 2 & 7 & 1 & 2 \\ 2 & 2 & 1 & 7 \end{pmatrix} = \begin{pmatrix} 67 & 52 & 31 & 72 \\ 31 & 21 & 13 & 31 \\ 52 & 37 & 21 & 52 \\ 72 & 52 & 31 & 67 \end{pmatrix}.$$

Inspired by this, one can try and count the number $C(n,b)$ of pairs of $n \times n$ matrices, whose entries are base b digits, such that their matrix multiplication is equal to their entry-wise digit concatenation. That is,

$$C(n,b) = \# \left\{ (A,B) \;\middle|\; \begin{array}{l} A, B \in \mathrm{Mat}_{n \times n}(\mathbb{Z}), \\ 0 \leq A_{i,j} < b, \; 0 \leq B_{i,j} < b, \\ AB = bA + B \end{array} \right\}.$$

The question is to get an asymptotic for this count, say when $b = 10$ and n is large.

Remark. *The asymptotics for $C(n, b)$ in the case where $n = 2$ and $b = p$ is a large prime are computed in Gal Benkler's master thesis (still umpublished) where she shows that*

$$C(2, p) = \frac{2}{\zeta(2)} p^2 + \frac{1}{2\zeta(2)} p(\log p)^2 + O(p \cdot \log p \cdot \log\log p).$$

4. Vivian Kuperberg

Denote $\mathrm{ord}_p(a)$ the order of a in $\mathbb{Z}/p\mathbb{Z}$. Show that $\mathrm{ord}_p(17) > \mathrm{ord}_p(2)$ for infinitely many primes p.

Remark. *In* [8] *Just and Pollack showed that* $\mathrm{ord}_p(n) > \mathrm{ord}_p(2)$ *for infinitely many primes p provided $n \not\equiv 1 \bmod 8$. They also showed that almost all n satisfy* $\mathrm{ord}_p(n) > \mathrm{ord}_p(2)$ *for infinitely many primes p.*

5. Efthymios Sofos - Question 1

Denote

$$h_4(d) = \#\mathrm{Cl}\left(\mathbb{Q}(\sqrt{d})\right)[4]$$

the size of the 4-torsion of the class group of $\mathbb{Q}(\sqrt{d})$.

Can one prove asymptotics for

$$\sum_{\substack{t \le X \\ 1+t^2 \text{ square free}}} h_4(1 + t^2)$$

or

$$\sum_{\substack{t \le X \\ t(t+1) \text{ square free}}} h_4(t(t + 1))?$$

6. Efthymios Sofos - Question 2

For a smooth, convex, positive curvature planar domain $\Omega \subset \mathbb{R}^2$, one can define the asymptotic density f_Ω for the normalized error term in the Ω lattice point counting problem by

$$\mathrm{prob}\left(r \in [0, R],\ \frac{|\mathbb{Z}^2 \cap (r\Omega)| - r^2 \mathrm{Area}(\Omega)}{\sqrt{r}} < z\right) \xrightarrow{R\to\infty} \int_{-\infty}^{z} f_\Omega(t) \mathrm{d}t.$$

In the above formula $r\Omega$ is the dilatation of Ω by a factor of r. Bleher computed these asymptotic distributions for various different shapes Ω, resulting in different asymptotic densities [2].

Inspired by this, one can look for similar asymptotic densities in a different problem - that of counting solutions to quadratics in 4 variables.

Let $Q(x_1, x_2, x_3, x_4)$ be a quadratic form. Is there an asymptotic density for

$$\frac{\#\left\{\underline{x} \in \mathbb{Z}^4 \cap [-r, r]^4 \ : \ Q(\underline{x}) = 0\right\} - \mathrm{MT}}{r}$$

where MT is an appropriate main term?

Remark. *An asymptotic for MT was obtained by the delta symbol circle method* [7] *and the secondary terms in the asymptotic were studied in* [6].

7. Mayank Pandey

Denote by K_{n_0,n_1,n_2,n_3} the splitting field of $n_0 + n_1x + n_2x^2 + n_3x^3$. The question is to provide bounds for

$$S(X) = \sum_{|n_0|,|n_1|,|n_2|,|n_3| \le X} \zeta_{K_{n_0,n_1,n_2,n_3}}\left(\frac{1}{2}\right)$$

where $\zeta_{K_{n_0,n_1,n_2,n_3}}$ is the Dedekind zeta function.

Using convexity estimate for each term individually, one can obtain $S(X) \ll X^5$. Applying known subconvexity bounds for each term can improve this to $S(X) \ll X^{5-1/3}$. The question is whether one can take advantage of the extra averaging over the n's to give a better bound.

8. Michael Stoll

Can one construct a sequence $(C_n)_{n\ge1}$ of nice curves over $\mathbb{Q}$ of genus $g(C_n) \ge 2$ such that

$$\lim_{n\to\infty} \frac{\#C_n(\mathbb{Q})}{g(C_n)} \to \infty?$$

Remark. *In* [3] *it was shown that the weak Lang conjecture implies that the number of rational points is bounded by a constant depending only on the genus. This would imply that if a sequence (C_n) as above exists, it must satisfy $g(C_n) \to \infty$. Recently, it was shown in* [4] *that the number of rational points is bounded in terms of the genus and the Mordell–Weil rank. And so, if one assumes that the Mordell–Weil rank is bounded, this too would imply that one must have $g(C_n) \to \infty$.*

References

[1] M. Bhargava, Galois groups of random integer polynomials and van der Waerden's conjecture, Ann. of Math. (2) **201** (2025), no. 2, 339–377.

[2] P. M. Bleher, Trace formula for quantum integrable systems, lattice-point problem, and small divisors, in *Emerging applications of number theory (Minneapolis, MN, 1996)*, 1–38, IMA Vol. Math. Appl., 109, Springer, New York.

[3] L. Caporaso, J. D. Harris and B. C. Mazur, Uniformity of rational points, J. Amer. Math. Soc. **10** (1997), no. 1, 1–35.

[4] V. Dimitrov, Z. Gao and P. Habegger, Uniformity in Mordell-Lang for curves, Ann. of Math. (2) **194** (2021), no. 1, 237–298.

[5] R. Dionisio, @ZahlenRMD, Jan 9, 2025, x.com/ZahlenRMD/status/1877348589774541213.

[6] J. R. Getz, Secondary terms in asymptotics for the number of zeros of quadratic forms over number fields, J. Lond. Math. Soc. (2) **98** (2018), no. 2, 275–305.

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

[8] M. Just and P. Pollack, Comparing multiplicative orders mod p, as p varies, New York J. Math. **27** (2021), 600–614.

[9] B. L. van der Waerden, Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt, Monatsh. Math. Phys. **43** (1936), no. 1, 133–147.

Reporter: Noam Kimmel

Participants

Prof. Dr. Lior Bary-Soroker
School of Mathematical Sciences
Tel Aviv University
Ramat Aviv, Tel Aviv 69978
ISRAEL

Or Ben-Porath
Department of Mathematics
School of Mathematical Sciences
Tel Aviv University
P.O. Box 39040
Ramat Aviv, Tel Aviv 69978
ISRAEL

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

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

Dr. Sam Chow
Mathematics Institute
University of Warwick
Zeeman Building
Coventry CV4 7AL
UNITED KINGDOM

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

Prof. Dr. Sary Drappeau
Laboratoire de Mathématiques Blaise
Pascal
UMR 6620 du CNRS
Université Clermont-Auvergne
63177 Aubière Cedex
FRANCE

Prof. Dr. Alexei Entin
Department of Mathematics
School of Mathematical Sciences
Tel Aviv University
P.O. Box 39040
Ramat Aviv, Tel Aviv 69978
ISRAEL

Prof. Dr. Arno Fehm
Institut für Algebra
Fakultät Mathematik
Technische Universität Dresden
01062 Dresden
GERMANY

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

Dr. Daniele Garzoni
Dept. of Mathematics, DRB 155
University of Southern California
1042 W 36th Place
Los Angeles, CA 90089-1113
UNITED STATES

David Hokken
Mathematisch Instituut
Universiteit Utrecht
Budapestlaan 6
P. O. Box 80.010
3508 TA Utrecht
NETHERLANDS

Noam Kimmel
Department of Mathematics
School of Mathematical Sciences
Tel Aviv University
P.O. Box 39040
Ramat Aviv, Tel Aviv 69978
ISRAEL

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

Dr. Peter Koymans
Mathematisch Instituut
Universiteit Utrecht
Budapestlaan 6
P. O. Box 80.010
3508 TA Utrecht
NETHERLANDS

Prof. Dr. Gady Kozma
Faculty of Mathematics and Computer Science
The Weizmann Institute of Science
P.O. Box 26
Rehovot 76100
ISRAEL

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

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

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

Johannes Linn
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
GERMANY

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

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

Prof. Dr. Philippe Gabriel Michel
Institut de Mathématiques
École Polytechnique Fédérale
de Lausanne
Station 8
1015 Lausanne
SWITZERLAND

Prof. Dr. Danny Neftin
Department of Mathematics
TECHNION
Israel Institute of Technology
Haifa 32000
ISRAEL

Prof. Dr. Alina Ostafe
The University of New South Wales
School of Mathematics and Statistics
Sydney NSW 2052
AUSTRALIA

Dr. Carlo Pagano
Dept. of Mathematics
Concordia University
1400 Maisonneuve Boulevard West
Montréal H3G 1M8
CANADA

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

Prof. Dr. Jennifer Park
Department of Mathematics
The Ohio State University
231 W 18th Ave
Columbus, OH 43215
UNITED STATES

Dr. Sun Woo Park
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
GERMANY

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

Dr. Brad Rodgers
Department of Mathematics
and Statistics
Queen's University
Jeffery Hall
Kingston ON K7L 3N6
CANADA

Prof. Dr. Peter C. Sarnak
School of Mathematics
Institute for Advanced Study
1 Einstein Drive
Princeton, NJ 08540
UNITED STATES

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

Prof. Dr. Igor E. Shparlinski
Department of Pure Mathematics
UNSW
Sydney NSW 2052
AUSTRALIA

Dr. Mark Shusterman
Department of Mathematics
The Weizmann Institute of Science
P. O. Box 26
Rehovot 76 100
ISRAEL

Prof. Dr. Alexei N. Skorobogatov
Department of Mathematics
Imperial College London
Huxley Building
180 Queen's Gate
London SW7 2AZ
UNITED KINGDOM

Dr. Efthymios Sofos
University of Rome "Tor Vergata"
Via della Ricerca Scientifica, 1
00133 Roma
ITALY

Prof. Dr. Cameron L. Stewart
Dept. of Pure Mathematics
University of Waterloo
200 University Avenue West
Waterloo N2L3G1
CANADA

Prof. Dr. Michael Stoll
Mathematisches Institut
Universität Bayreuth
95440 Bayreuth
GERMANY

Dr. Ashvin A. Swaminathan
Department of Mathematics
Harvard University
Science Center
One Oxford Street
Cambridge MA 02138-2901
UNITED STATES

Dr. Niclas Technau
Department of Mathematics
University of Wisconsin-Madison
480 Lincoln Drive
Madison, WI 53706-1388
UNITED STATES

Prof. Dr. Evelina Viada
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstr. 3-5
37073 Göttingen
GERMANY

Dr. Victor Wang
Institute of Science and Technology
Austria (ISTA)
Am Campus 1
3400 Klosterneuburg
AUSTRIA

Katharine Woo
Department of Mathematics
Stanford University
Stanford CA 94305-2125
UNITED STATES

Prof. Dr. Melanie Matchett Wood
Department of Mathematics
Harvard University
02138 Cambridge
UNITED STATES

Dr. Max Wenqiang Xu
Courant Institute
NYU
251 Mercer St
New York NY 10012
UNITED STATES