Some quadratic counting problems

Victor Wang
(based on work of many authors)

IST Austria and Institute of Mathematics, Academia Sinica

N-Cube Days XXII, Stockholm University, June 2025

This project has received funding from the European Union's Horizon 2020 research and innovation program

under the Marie Skłodowska-Curie Grant Agreement No. 101034413

Integer points on log K3 surfaces

The Markov-type surface $x^2 + y^2 + z^2 - xyz = k$ is *log Calabi–Yau*. We are interested in solutions $(x, y, z) \in \mathbb{Z}^3$.

- Heuristically, expect only $O_k((\log B)^2)$ solutions with $\max(|x|, |y|, |z|) \leq B$, as $B \to \infty$. More generally, see conjectures of [Browning–Wilsch 2024].
- Such Diophantine equations lie at the boundary between heuristic solubility and paucity. Any integer solutions only barely exist (on average)!

Integer points on log K3 surfaces

The Markov-type surface $x^2 + y^2 + z^2 - xyz = k$ is *log Calabi–Yau*. We are interested in solutions $(x, y, z) \in \mathbb{Z}^3$.

- Heuristically, expect only $O_k((\log B)^2)$ solutions with $\max(|x|, |y|, |z|) \leq B$, as $B \to \infty$. More generally, see conjectures of [Browning–Wilsch 2024].
- Such Diophantine equations lie at the boundary between heuristic solubility and paucity. Any integer solutions only barely exist (on average)!
- Another, infamous, example of a log K3 surface is the *sum of 3 cubes* problem $x^3 + y^3 + z^3 = k$. For $k = 42$ the only known solution [Booker–Sutherland 2019] is

$$(-80538738812075974)^3+(80435758145817515)^3+(126021232$$

- These problems test the limits of our understanding.
- They are directly adjacent to undecidable problems. ($\exists$ undecidable quartic equations over $\mathbb{Z}$.)

Solubility of Markov-type surfaces

The polynomial $M = x^2 + y^2 + z^2 - xyz$ is fixed by a group $\Gamma \subseteq \mathrm{Aut}(M)$, where Γ is formed by S_3, sign changes ± 1, and Vieta involutions $(x, y, z) \mapsto (x, y, xy - z)$. Let $h_M(k)$ be the number of Γ-orbits of the set $\{(x, y, z) \in \mathbb{Z}^3 : M = k\}$.

Theorem (Ghosh–Sarnak 2017)

We have $h_M(k) \to \infty$ along a density 1 of admissible[a] $k \in \mathbb{Z}$. In particular, the integral Hasse principle holds for almost all $k \in \mathbb{Z}$.

[a] $k \not\equiv 3 \bmod 4$ and $k \not\equiv \pm 3 \bmod 9$

Solubility of Markov-type surfaces

The polynomial $M = x^2 + y^2 + z^2 - xyz$ is fixed by a group $\Gamma \subseteq \mathrm{Aut}(M)$, where Γ is formed by S_3, sign changes ± 1, and Vieta involutions $(x, y, z) \mapsto (x, y, xy - z)$. Let $h_M(k)$ be the number of Γ-orbits of the set $\{(x, y, z) \in \mathbb{Z}^3 : M = k\}$.

Theorem (Ghosh–Sarnak 2017)

We have $h_M(k) \to \infty$ along a density 1 of admissible[a] $k \in \mathbb{Z}$. In particular, the integral Hasse principle holds for almost all $k \in \mathbb{Z}$.

[a] $k \not\equiv 3 \bmod 4$ and $k \not\equiv \pm 3 \bmod 9$

Theorem (Mishra 2024; lower bound is new)

Fix $\epsilon > 0$. The inequality $(\log |k|)^{2-\epsilon} \leq h_M(k) \leq (\log |k|)^{2+\epsilon}$ holds for a density 1 of admissible $k \in \mathbb{Z}$.

(Upper bound $\Leftarrow$ Ghosh–Sarnak + Markov's inequality.)

For all $k < 0$ (and for all "generic" $k \geq 5$), Ghosh–Sarnak construct a fundamental domain $\mathcal{F}_k$ for the action of Γ on $\{(x, y, z) \in \mathbb{Z}^3 : x^2 + y^2 + z^2 - xyz = k\}$. Let $r_M(k)$ be the number of points in a well-chosen region $\mathcal{F}'_k \subseteq \mathcal{F}_k$.

- For Ghosh–Sarnak, $\mathcal{F}'_k$ satisfies $|x| \asymp |yz| \asymp |k|^{1/2}$ and $|z| \leq |k|^{\epsilon}$. Real density of solutions: $\sigma_\infty(k) \asymp \epsilon \log |k|$.
- For Mishra, $\mathcal{F}'_k$ is part of a $\mathbb{G}_m^2$-torus $|xyz| \asymp |k|$, with $|k|^{\delta} \leq |x/y| \leq |k|^{-\delta}|z| \leq |k|^{2\delta}$. Here $\sigma_\infty(k) \asymp (\log |k|)^2$.

For all $k < 0$ (and for all "generic" $k \geq 5$), Ghosh–Sarnak construct a fundamental domain $\mathcal{F}_k$ for the action of Γ on $\{(x, y, z) \in \mathbb{Z}^3 : x^2 + y^2 + z^2 - xyz = k\}$. Let $r_M(k)$ be the number of points in a well-chosen region $\mathcal{F}'_k \subseteq \mathcal{F}_k$.

- For Ghosh–Sarnak, $\mathcal{F}'_k$ satisfies $|x| \asymp |yz| \asymp |k|^{1/2}$ and $|z| \leq |k|^{\epsilon}$. Real density of solutions: $\sigma_\infty(k) \asymp \epsilon \log |k|$.
- For Mishra, $\mathcal{F}'_k$ is part of a $\mathbb{G}_m^2$-torus $|xyz| \asymp |k|$, with $|k|^{\delta} \leq |x/y| \leq |k|^{-\delta}|z| \leq |k|^{2\delta}$. Here $\sigma_\infty(k) \asymp (\log |k|)^2$.

One then expands and upper-bounds an *arithmetic variance*

$$Var(K, A) := \sum_{k \leq K} (r_M(k) - r_M^{loc}(k; A))^2.$$

- The sum $\sum_{k \leq K} r_M(k)^2$ counts solutions in a region to $x^2 + y^2 + z^2 - xyz = u^2 + v^2 + w^2 - uvw$.
- Here $r_M^{loc}(k; A)$ is roughly a truncated L-function at 1. Ghosh–Sarnak (resp. Mishra) use a multiplicative (resp. additive) truncation.
- Some of this generalizes to sums of three cubes.

Let $L(s, \boldsymbol{c})$ be the L-function of $V_{\boldsymbol{c}} : x_1^3 + \cdots + x_6^3 = \boldsymbol{c} \cdot \boldsymbol{x} = 0$, where $\boldsymbol{c} = (c_1, \ldots, c_6) \in \mathbb{F}_q[t]^6$, with $\gcd(q, 6) = 1$ and $\Delta(\boldsymbol{c}) := \operatorname{disc}(V_{\boldsymbol{c}}) = \prod(c_1^{3/2} \pm c_2^{3/2} \pm \cdots \pm c_6^{3/2}) \neq 0$.

Theorem (Browning–Glas–W. 2024)

Assume sufficient progress on moments of $\frac{1}{L(s,\boldsymbol{c})}$ *for* $\Delta(\boldsymbol{c}) \neq 0$. *Then* $x^3 + y^3 + z^3 = n$ *is soluble in elements* $x, y, z \in \mathbb{F}_q[t]$ *of degree* $\sim \frac{1}{3} \deg n$ *for a density* 1 *of elements* $n \in \mathbb{F}_q[t]$.

Let $L(s, \boldsymbol{c})$ be the L-function of $V_{\boldsymbol{c}} : x_1^3 + \cdots + x_6^3 = \boldsymbol{c} \cdot \boldsymbol{x} = 0$, where $\boldsymbol{c} = (c_1, \ldots, c_6) \in \mathbb{F}_q[t]^6$, with $\gcd(q, 6) = 1$ and $\Delta(\boldsymbol{c}) := \operatorname{disc}(V_{\boldsymbol{c}}) = \prod(c_1^{3/2} \pm c_2^{3/2} \pm \cdots \pm c_6^{3/2}) \neq 0$.

Theorem (Browning–Glas–W. 2024)

Assume sufficient progress on moments of $\frac{1}{L(s,\boldsymbol{c})}$ *for* $\Delta(\boldsymbol{c}) \neq 0$. *Then* $x^3 + y^3 + z^3 = n$ *is soluble in elements* $x, y, z \in \mathbb{F}_q[t]$ *of degree* $\sim \frac{1}{3} \deg n$ *for a density* 1 *of elements* $n \in \mathbb{F}_q[t]$.

Builds on ideas of many authors, such as the following:

- Ghosh–Sarnak, Diaconu (log-K3 variance analysis),
- Kloosterman, Hooley 1986, Heath-Brown,
- Beauville (quadric bundles over $\mathbb{P}^2$), Getz, Tran,
- Rubinstein–Sarnak (Chebyshev's bias via prime squares),
- Deligne (GRH), Hooley 1994 (singular cubics),
- Huang ($\approx \mathbb{Q}$-points), Busé–Jouanolou ($\Delta \in (f, (f')^2)$),
- Bhargava (Ekedahl sieve), Poonen (square-free sieve),
- Kisin (local constancy of L-factors).

What kind of progress on L-functions?

Let $2 \nmid q$. Let $\mu(r)$ be the Möbius function over $\mathbb{F}_q[t]$, and let $\chi_m(r) = (\frac{r}{m})$ be the Jacobi symbol over $\mathbb{F}_q[t]$.

Theorem (Bergström–Diaconu–Petersen–Westerland, Miller–Patzt–Petersen–Randal-Williams, W. 2024)

If $1 \leq M = 2g+1$ *and* $1 \leq R \leq \alpha M$, *and* $q \ggg_\alpha 1$, *then*

$$\frac{\sum_{|m|=q^M} \sum_{|r|=q^R} \mu(r)\chi_m(r)}{q^M q^{R/2}} \ll q^{-0.001M+O(1)},$$

where the sums over m *and* r *run through square-free, monic* $m, r \in \mathbb{F}_q[t]$ *with* $\deg m = M$ *and* $\deg r = R$, *respectively.*

Theorem (Same papers; new for $q = p \equiv 1 \bmod 4$)

The set $\{m : L(\frac{1}{2}, \chi_m) = 0\}$ *has upper density* $o_{q\to\infty}(1)$.

Deterministic versus random behavior

Many problems in analytic number theory concern the behavior of families of arithmetic sums, such as the family

$$\chi \mapsto \sum_{1 \le n \le x} \chi(n)$$

indexed by Dirichlet characters χ modulo a prime r, for some set of x. Defining properties of χ are *multiplicativity*

$$\chi(mn) = \chi(m)\chi(n), \qquad \chi(1) = 1, \qquad \chi(0) = 0,$$

and *periodicity*

$$\chi(n + r) = \chi(n).$$

Deterministic versus random behavior

Many problems in analytic number theory concern the behavior of families of arithmetic sums, such as the family

$$\chi \mapsto \sum_{1 \le n \le x} \chi(n)$$

indexed by Dirichlet characters χ modulo a prime r, for some set of x. Defining properties of χ are *multiplicativity*

$$\chi(mn) = \chi(m)\chi(n), \qquad \chi(1) = 1, \qquad \chi(0) = 0,$$

and *periodicity*

$$\chi(n + r) = \chi(n).$$

There are $|(\mathbb{Z}/r\mathbb{Z})^\times| = r - 1$ characters χ mod r. If r is large, then one might expect $\{\chi \bmod r\}$ to exhibit random behavior.

Deterministic versus random behavior (cont'd)

There are $|(\mathbb{Z}/r\mathbb{Z})^\times| = r-1$ characters χ mod r. If r is large, then one might expect $\{\chi \bmod r\}$ to exhibit random behavior. A useful random model (Steinhaus) for $\{\chi \bmod r\}$ is the family of *random multiplicative functions* $f : \mathbb{N} \to \mathbb{C}$,

$$f(mn) = f(m)f(n), \qquad f(1) = 1, \qquad |f(p)| = 1,$$

with $f(p)$ randomly (iid) drawn from $S^1 \subset \mathbb{C}$ for each prime p.

Deterministic versus random behavior (cont'd)

There are $|(\mathbb{Z}/r\mathbb{Z})^\times| = r-1$ characters χ mod r. If r is large, then one might expect $\{\chi \bmod r\}$ to exhibit random behavior. A useful random model (Steinhaus) for $\{\chi \bmod r\}$ is the family of *random multiplicative functions* $f : \mathbb{N} \to \mathbb{C}$,

$$f(mn) = f(m)f(n), \qquad f(1) = 1, \qquad |f(p)| = 1,$$

with $f(p)$ randomly (iid) drawn from $S^1 \subset \mathbb{C}$ for each prime p. The advantage of random multiplicative functions (rmf) is that

$$\mathbb{E}_f f(m)\overline{f}(n) = \mathbf{1}_{m=n}$$

(orthogonality) holds for all $m, n \geq 1$, whereas (by periodicity)

$$\mathbb{E}_{\chi \bmod r} \chi(m)\overline{\chi}(n) = \mathbf{1}_{m=n}$$

holds only in ranges such as $1 \leq m, n < r$.

Mixed character sums

Fix a smooth function $w\colon \mathbb{R} \to \mathbb{R}$, supported on $[0,1]$, with $\int_0^1 w(t)^2\,dt > 0$. We consider the *mixed character sum*

$$S(\chi,\theta;x) := \sum_{n\in\mathbb{Z}} \chi(n)e(n\theta)w(n/x) = \sum_{1\le n\le x} \chi(n)e(n\theta)w(n/x),$$

featuring a multiplicative character χ mod r and an additive character $e(n\theta) := \exp(2\pi i n\theta)$.

Mixed character sums

Fix a smooth function $w\colon \mathbb{R} \to \mathbb{R}$, supported on $[0,1]$, with $\int_0^1 w(t)^2\,dt > 0$. We consider the *mixed character sum*

$$S(\chi,\theta;x) := \sum_{n\in\mathbb{Z}} \chi(n)e(n\theta)w(n/x) = \sum_{1\le n\le x} \chi(n)e(n\theta)w(n/x),$$

featuring a multiplicative character χ mod r and an additive character $e(n\theta) := \exp(2\pi i n\theta)$.

Question

Fix $\theta \in \mathbb{R}$. Assume $1 \le x \le r$. How does $S(\chi,\theta;x)$ behave as χ mod r varies?

[Harper 2023] (building on [Harper 2020]) implies, for $\theta \in \mathbb{Q}$,

$$\mathbb{E}_{\chi \bmod r}|S(\chi,\theta;x)| = O(x^{1/2}/(\log\log\min(x,r/x))^{1/4}) = o(x^{1/2})$$

if $\min(x,r/x) \to \infty$, even for piecewise continuous w. I will discuss joint work with Max Xu (2024) concerning $\theta \notin \mathbb{Q}$.

Mixed character sums (rmf model)

For random multiplicative f let

$$S^\sharp(f,\theta;x) := \sum_{1\le n\le x} f(n)e(n\theta).$$

Fix $\theta \in \mathbb{R}$. How does $S^\sharp(f,\theta;x)$ behave as f varies?

Theorem (Harper 2020)

If $\theta \in \mathbb{Q}$ and $x \to \infty$, then $\mathbb{E}_f|S^\sharp(f,\theta;x)| = o(x^{1/2})$.

Theorem (Soundararajan–Xu 2023)

Suppose $\|q\theta\| := \min_{a\in\mathbb{Z}}|q\theta - a| \gg \exp(-q^{1/50})$ for all $q \in \mathbb{N}$.[a] Then as $x \to \infty$, the random variable $S^\sharp(f,\theta;x)/x^{1/2}$ converges in distribution to the standard complex Gaussian $\mathcal{CN}(0,1)$. Moreover, $\mathbb{E}_f|S^\sharp(f,\theta;x)| \sim cx^{1/2}$ $(c > 0)$.

[a] This is satisfied for most $\theta \in \mathbb{R}$, including π, e, and any algebraic irrational θ. For most $\theta \in \mathbb{R}$, we have $\|q\theta\| \gg q^{-1-\epsilon}$ for all $q \in \mathbb{N}$.

Mixed character sums (deterministic)

Fix a smooth function $w\colon \mathbb{R} \to \mathbb{R}$, supported on $[0,1]$, with $\int_0^1 w(t)^2\,dt > 0$. For characters χ mod r let

$$S(\chi,\theta;x) := \sum_{n\in\mathbb{Z}} \chi(n)e(n\theta)w(n/x) = \sum_{1\le n\le x} \chi(n)e(n\theta)w(n/x).$$

Fix $\theta \in \mathbb{R}$. Assume $1 \le x \le r$.

Theorem (Harper 2023)

If $\theta \in \mathbb{Q}$, then $\mathbb{E}_{\chi \bmod r}|S(\chi,\theta;x)| = o(x^{1/2})$ as $\min(x, r/x) \to \infty$, even for piecewise continuous w.

Theorem (W.–Xu 2024)

Suppose $\|q\theta\| := \min_{a\in\mathbb{Z}}|q\theta - a| \gg \exp(-q^{1/4})$ for all $q \in \mathbb{N}$. If $x \ggg 1$, then $x^{1/2} \ll \mathbb{E}_{\chi \bmod r}|S(\chi,\theta;x)| \ll x^{1/2}$.

Second moment

For $1 \leq x \leq r$, orthogonality over $\{\chi \bmod r\}$ implies that

$$\mathbb{E}_\chi \Big| \sum_{1 \leq n \leq x} \chi(n) e(n\theta) w(n/x) \Big|^2 = \sum_{1 \leq n \leq \min(x, r-1)} w(n/x)^2$$
$$\sim x \int_0^1 w(t)^2 \, dt \asymp x,$$

provided that x is sufficiently large (in terms of w).

Second moment

For $1 \le x \le r$, orthogonality over $\{\chi \bmod r\}$ implies that

$$\mathbb{E}_\chi \Big| \sum_{1 \le n \le x} \chi(n) e(n\theta) w(n/x) \Big|^2 = \sum_{1 \le n \le \min(x, r-1)} w(n/x)^2$$
$$\sim x \int_0^1 w(t)^2 \, dt \asymp x,$$

provided that x is sufficiently large (in terms of w). Thus

$$\mathbb{E}_{\chi \bmod r} |S(\chi, \theta; x)| = \mathbb{E}_\chi \Big| \sum_{1 \le n \le x} \chi(n) e(n\theta) w(n/x) \Big| \ll x^{1/2}$$

by Cauchy–Schwarz over $\{\chi \bmod r\}$. Thus the desired upper bound in [W.–Xu 2024] holds without any Diophantine condition on $\theta \in \mathbb{R}$. The lower bound is the interesting part.

Fourth moment

By Hölder's inequality,

$$(\mathbb{E}_\chi|S(\chi,\theta;x)|)^2(\mathbb{E}_\chi|S(\chi,\theta;x)|^4) \geq (\mathbb{E}_\chi|S(\chi,\theta;x)|^2)^3 \gg x^3,$$

so the desired lower bound $\mathbb{E}_\chi|S(\chi,\theta;x)| \gg x^{1/2}$ will follow if we can show that

$$\mathbb{E}_\chi|S(\chi,\theta;x)|^4 \ll x^2.$$

Fourth moment

By Hölder's inequality,

$$(\mathbb{E}_\chi|S(\chi,\theta;x)|)^2(\mathbb{E}_\chi|S(\chi,\theta;x)|^4) \geq (\mathbb{E}_\chi|S(\chi,\theta;x)|^2)^3 \gg x^3,$$

so the desired lower bound $\mathbb{E}_\chi|S(\chi,\theta;x)| \gg x^{1/2}$ will follow if we can show that

$$\mathbb{E}_\chi|S(\chi,\theta;x)|^4 \ll x^2.$$

If $x \leq r^{1/2}$, then orthogonality over χ gives (for some smooth weight W, which is not important)

$$\begin{aligned}\mathbb{E}_\chi|S(\chi,\theta;x)|^4 &= \sum_{\substack{1\leq m_1,m_2,n_1,n_2\leq x\\ m_1m_2=n_1n_2}} e((m_1+m_2-n_1-n_2)\theta)W \\ &= \mathbb{E}_f|S(f,\theta;x)|^4 \ll x^2,\end{aligned}$$

by the methods of [Soundararajan–Xu 2023]. (Parameterize solutions; combinatorially decompose into geometric series.)

If $x \geq r^{1/2}$, then $m_1 m_2 \equiv n_1 n_2 \bmod r$ is no longer equivalent to $m_1 m_2 = n_1 n_2$. Thus, we choose not to directly compute the fourth moment as we did for $x \leq r^{1/2}$. Instead, we study a dual problem, with r/x replacing x.

If $x \geq r^{1/2}$, then $m_1 m_2 \equiv n_1 n_2 \bmod r$ is no longer equivalent to $m_1 m_2 = n_1 n_2$. Thus, we choose not to directly compute the fourth moment as we did for $x \leq r^{1/2}$. Instead, we study a dual problem, with r/x replacing x. Write $\theta = \frac{k}{r} + \theta'$, where $k = \lfloor r\theta \rfloor \in \mathbb{Z}$ and $0 \leq \theta' < 1/r$. We define

$$f_{r,\chi}(n) := \chi(n) e(\frac{kn}{r}), \quad f_\infty(n) := w(\frac{n}{x}) e(n\theta').$$

Then $S(\chi, \theta; x)$ may be written as

$$\sum_{n \in \mathbb{Z}} \chi(n) e(n\theta) w(\frac{n}{x}) = \sum_{n \in \mathbb{Z}} f_{r,\chi}(n) f_\infty(n) = \sum_{m \in \mathbb{Z}} \hat{f}_{r,\chi}(\frac{m}{r}) \hat{f}_\infty(\frac{m}{r})$$

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

$$\hat{f}_{r,\chi}(\frac{m}{r}) = \frac{1}{r} \sum_{a \in \mathbb{Z}/r\mathbb{Z}} \chi(a) e\left(\frac{(k+m)a}{r}\right)$$

and $\hat{f}_\infty(\frac{m}{r}) = \int_{\mathbb{R}} w(\frac{t}{x}) e((\theta' - \frac{m}{r})t) dt$.

Fourier coefficients

We now estimate the Fourier coefficients $\hat{f}_{r,\chi}(\frac{m}{r})$ and $\hat{f}_{\infty}(\frac{m}{r})$. If $k+m \not\equiv 0 \bmod r$, then by standard properties of Gauss sums,

$$\hat{f}_{r,\chi}(\frac{m}{r}) = \frac{1}{r}\sum_{a\in\mathbb{Z}/r\mathbb{Z}} \chi(a)e\left(\frac{(k+m)a}{r}\right) = \chi(k+m)^{-1}\frac{C(\chi)}{r^{1/2}},$$

where $|C(\chi)| \leq 1$ and $C(\chi)$ depends only on χ. Moreover, integration by parts over $t \in \mathbb{R}$ gives

$$\hat{f}_{\infty}(\frac{m}{r}) = \int_{\mathbb{R}} w(\frac{t}{x})e((\theta'-\frac{m}{r})t)dt \ll_A x\big(1+\frac{x\max(|m|-1,0)}{r}\big)^{-A}$$

for all $A \geq 0$, using smoothness of w.

Fourier coefficients

We now estimate the Fourier coefficients $\hat{f}_{r,\chi}(\frac{m}{r})$ and $\hat{f}_{\infty}(\frac{m}{r})$. If $k+m \not\equiv 0 \bmod r$, then by standard properties of Gauss sums,

$$\hat{f}_{r,\chi}(\frac{m}{r}) = \frac{1}{r}\sum_{a\in\mathbb{Z}/r\mathbb{Z}} \chi(a)e\left(\frac{(k+m)a}{r}\right) = \chi(k+m)^{-1}\frac{C(\chi)}{r^{1/2}},$$

where $|C(\chi)| \leq 1$ and $C(\chi)$ depends only on χ. Moreover, integration by parts over $t \in \mathbb{R}$ gives

$$\hat{f}_{\infty}(\frac{m}{r}) = \int_{\mathbb{R}} w(\frac{t}{x})e((\theta'-\frac{m}{r})t)dt \ll_A x\big(1+\frac{x\max(|m|-1,0)}{r}\big)^{-A}$$

for all $A \geq 0$, using smoothness of w. Plugging this into $S(\chi,\theta;x) = \sum_{m\in\mathbb{Z}} \hat{f}_{r,\chi}(\frac{m}{r})\hat{f}_{\infty}(\frac{m}{r})$, we morally get

$$|S(\chi,\theta;x)| \approx |\sum_{\substack{|m|\leq 2+r/x \\ m\not\equiv -k \bmod r}} \frac{\chi(k+m)^{-1}}{r^{1/2}}x|.$$

Orthogonality after duality

We are essentially left with proving that

$$\mathbb{E}_\chi \Big| \sum_{\substack{|m| \le 2 + r/x \\ m \not\equiv -k \bmod r}} \frac{\chi(k+m)^{-1}}{r^{1/2}} x \Big|^4 \ll x^2.$$

Orthogonality after duality

We are essentially left with proving that

$$\mathbb{E}_\chi \Big| \sum_{\substack{|m|\le 2+r/x \\ m\not\equiv -k \bmod r}} \frac{\chi(k+m)^{-1}}{r^{1/2}} x \Big|^4 \ll x^2.$$

By orthogonality, LHS $= \frac{x^4}{r^2}\mathcal{N}_4(2+r/x)$, where $\mathcal{N}_4(T)$ counts integer solutions

$$(m_1, m_2, n_1, n_2) \in \{|m| \le T : m \not\equiv -k \bmod r\}^4$$

to the congruence

$$(k+m_1)(k+m_2) \equiv (k+n_1)(k+n_2) \bmod r.$$

This congruence is equivalent to

$$k(m_1+m_2-n_1-n_2) \equiv n_1 n_2 - m_1 m_2 \bmod r.$$

We want to prove $\mathcal{N}_4(T) \ll T^2$ for $3 \le T \le 2 + r^{1/2}$.

Write $S = m_1 + m_2 - n_1 - n_2$ and $P = n_1 n_2 - m_1 m_2$.

Lemma (Almost a parameterization of solutions)

There exists a linear map $\Phi\colon \mathbb{Z}^4 \to \mathbb{Z}^3$ such that if $S, P \in \mathbb{Z}$, then Φ maps the set $\mathcal{A}$ injectively into the set $\mathcal{B}$, where

$$\mathcal{A} := \{(m_1, m_2, n_1, n_2) \in \mathbb{Z}^4 : m_1 + m_2 - n_1 - n_2 = S, \\ n_1 n_2 - m_1 m_2 = P\},$$

$$\mathcal{B} := \{(a, b, c) \in \mathbb{Z}^3 : ab + 2cS = S^2 - 4P\}.$$

Write $S = m_1 + m_2 - n_1 - n_2$ and $P = n_1 n_2 - m_1 m_2$.

Lemma (Almost a parameterization of solutions)

There exists a linear map $\Phi\colon \mathbb{Z}^4 \to \mathbb{Z}^3$ such that if $S, P \in \mathbb{Z}$, then Φ maps the set $\mathcal{A}$ injectively into the set $\mathcal{B}$, where

$$\mathcal{A} := \{(m_1, m_2, n_1, n_2) \in \mathbb{Z}^4 : m_1 + m_2 - n_1 - n_2 = S, \\ n_1 n_2 - m_1 m_2 = P\},$$

$$\mathcal{B} := \{(a, b, c) \in \mathbb{Z}^3 : ab + 2cS = S^2 - 4P\}.$$

Proof.

Let $\Phi(m_1, m_2, n_1, n_2) := (a, b, c)$ where

$$(a, b, c) := (n_1 - n_2 + m_1 - m_2, n_1 - n_2 - m_1 + m_2, m_1 + m_2).$$

Then $ab + c^2 = (c - S)^2 - 4P$. Therefore, Φ maps $\mathcal{A}$ into $\mathcal{B}$. Moreover, this map is injective, because the linear forms a, b, c, S are linearly independent over $\mathbb{Q}$. □

Fibering $\mathcal{N}_4(T)$ over (S, P)

We want to prove $\mathcal{N}_4(T) \ll T^2$ for $3 \leq T \leq 2 + r^{1/2}$, where $\mathcal{N}_4(T)$ counts certain solutions to the congruence

$$kS \equiv P \bmod r.$$

By the lemma, we have

$$\mathcal{N}_4(T) \leq \sum_{\substack{|S| \leq 4T,\ |P| \leq 2T^2 \\ kS \equiv P \bmod r}} N_{S,P}(T),$$

where

$$N_{S,P}(T) := \#\{a, b, c \ll T : ab + 2cS = S^2 - 4P\}.$$

Fibering $\mathcal{N}_4(T)$ over (S, P)

We want to prove $\mathcal{N}_4(T) \ll T^2$ for $3 \leq T \leq 2 + r^{1/2}$, where $\mathcal{N}_4(T)$ counts certain solutions to the congruence

$$kS \equiv P \bmod r.$$

By the lemma, we have

$$\mathcal{N}_4(T) \leq \sum_{\substack{|S| \leq 4T,\ |P| \leq 2T^2 \\ kS \equiv P \bmod r}} N_{S,P}(T),$$

where

$$N_{S,P}(T) := \#\{a, b, c \ll T : ab + 2cS = S^2 - 4P\}.$$

The equation $ab + 2cS = S^2 - 4P$ implies that

$$ab + 4P \equiv 0 \bmod S, \qquad ab + 4P \ll TS + S^2 \ll TS,$$

since $c \ll T$ and $S \ll T$. Therefore,

$$N_{S,P}(T) \leq \#\{a, b \ll T : S \mid ab + 4P, \quad ab + 4P \ll TS\}.$$

Lemma (Hyperbolic summation in a residue class)

Suppose $1 \le u, v \le S \ll T$. *Then*

$$\sum_{\substack{a,b \ll T \\ (a,b) \equiv (u,v) \bmod S}} \mathbf{1}_{ab+4P \ll TS} \ll \frac{T}{S} \log(2 + \frac{T}{S}).$$

Proof idea.

Given a, we may accurately count integers $b \equiv v \bmod S$ in any interval of length $\min(T, TS/|a|) \gg S$, since $a \ll T$. □

For any $S \ll T$ with $S \neq 0$, the lemma implies

$$N_{S,P}(T) \le \sum_{a,b \ll T} \mathbf{1}_{S|ab+4P} \mathbf{1}_{ab+4P \ll TS} \ll \frac{T}{|S|} \log(2+\frac{T}{|S|}) N(-4P, S),$$

where $N(d, q) := \#\{(a, b) \in (\mathbb{Z}/q\mathbb{Z})^2 : ab \equiv d \bmod q\}$.

We bound $N(d,q) := \#\{(a,b) \in (\mathbb{Z}/q\mathbb{Z})^2 : ab \equiv d \bmod q\}$.

Lemma (Counting residue classes)

Let $d \in \mathbb{Z}$ and $q \in \mathbb{N}$. Then $N(d,q) \leq \tau(\gcd(d,q))q$, where $\tau(\cdot)$ is the divisor function.

Proof.

It suffices to prove the lemma when q is a prime power. Say $q = p^t$ and $\gcd(d,q) = p^m$. Then clearly $t \geq m \geq 0$. If $m = 0$, then

$$N(d,q) = \phi(q) \leq q.$$

If $m = 1$, then $N(d,q) = 2\phi(q) + \mathbf{1}_{t=1} \leq 2q$. If $m \geq 2$, then

$$N(d,q) = 2\phi(q) + p^2 N(d/p^2, q/p^2).$$

By induction on m, it follows that $N(d,q) \leq (m+1)q$. □

Dyadic fibering over gcd

For any $S \ll T$ with $S \neq 0$, the lemma implies

$$N_{S,P}(T) \ll \frac{T}{|S|} \log(2 + \frac{T}{|S|}) N(-4P, S)$$
$$\ll T \log(2 + \frac{T}{|S|}) \tau(\gcd(P, S)),$$

Dyadic fibering over gcd

For any $S \ll T$ with $S \neq 0$, the lemma implies

$$N_{S,P}(T) \ll \frac{T}{|S|} \log(2 + \frac{T}{|S|}) N(-4P, S)$$
$$\ll T \log(2 + \frac{T}{|S|}) \tau(\gcd(P, S)),$$

Upon writing $(S, P) = (gS', gP')$ with $g = \gcd(S, P) \geq 1$, and summing $\tau(g)$ over dyadic intervals $[G/2, G)$, we get (ignoring the $S = 0$ contribution, which is easy to deal with)

$$\mathcal{N}_4(T) \leq \sum_{\substack{|S| \leq 4T,\ |P| \leq 2T^2 \\ kS \equiv P \bmod r}} N_{S,P}(T)$$

$$\ll \sum_{\substack{G \in \{2,4,8,\ldots\} \\ G \ll T}} \sum_{\substack{S' \ll T/G,\ P' \ll T^2/G \\ kS' \equiv P' \bmod r}} T \log(2 + \frac{T}{|GS'|})(G \log G).$$

Lemma (Pigeonhole counting bound)

Assume $|q\theta - a| \gg \Upsilon(q)$ *for all* $(a, q) \in \mathbb{Z} \times \mathbb{N}$, *where* Υ *is a decreasing, nonnegative function. If* $\frac{r}{2} > M \geq N \geq 1$, *then*

$$\Upsilon\left(\frac{N}{\#\{(S', P') \in [1, N] \times [-M, M] : kS' \equiv P' \bmod r\}}\right) \ll \frac{M}{r}.$$

Lemma (Pigeonhole counting bound)

Assume $|q\theta - a| \gg \Upsilon(q)$ *for all* $(a, q) \in \mathbb{Z} \times \mathbb{N}$, *where* Υ *is a decreasing, nonnegative function. If* $\frac{r}{2} > M \geq N \geq 1$, *then*

$$\Upsilon\left(\frac{N}{\#\{(S', P') \in [1, N] \times [-M, M] : kS' \equiv P' \bmod r\}}\right) \ll \frac{M}{r}.$$

Proof.

By pigeonhole, there exists $(q, d) \in [1, N] \times [-2M, 2M]$ such that $kq \equiv d \bmod r$ and $q \leq \frac{N}{\#\{(S',P') \in [1,N] \times [-M,M] : kS' \equiv P' \bmod r\}}$. For such a pair (q, d), we have $kq = d + ra$ for some $a \in \mathbb{Z}$. But by definition of k, we have $|r\theta - k| < 1$. Therefore,

$$|qr\theta - ra| \leq |qr\theta - kq| + |kq - ra| < q + |d| \leq N + 2M \leq 3M,$$

whence $|q\theta - a| \leq 3M/r$. Yet by assumption, $|q\theta - a| \gg \Upsilon(q)$. Since $\Upsilon(q)$ is decreasing, the lemma follows. □

Applying the lemma

If $\frac{r}{2} > M \geq N \geq 1$ and $\Upsilon(q) = \exp(-q^{1/3})$, then

$$\#\{S' \ll N,\ P' \ll M : kS' \equiv P' \bmod r\} \ll \frac{N}{(\log(2 + r/M))^3}$$

by the lemma; this is also trivially true if $M \asymp r$.

Applying the lemma

If $\frac{r}{2} > M \geq N \geq 1$ and $\Upsilon(q) = \exp(-q^{1/3})$, then

$$\#\{S' \ll N,\ P' \ll M : kS' \equiv P' \bmod r\} \ll \frac{N}{(\log(2 + r/M))^3}$$

by the lemma; this is also trivially true if $M \asymp r$. Thus

$$\mathcal{N}_4(T) \ll \sum_{\substack{G \in \{2,4,8,\dots\} \\ G \ll T}} \sum_{\substack{S' \ll T/G,\ P' \ll T^2/G \\ kS' \equiv P' \bmod r}} T \log(2 + \frac{T}{|GS'|})(G \log G)$$

$$\ll \sum_{\substack{G,N \in \{2,4,8,\dots\} \\ GN \ll T}} T \log(2 + \frac{T}{|GN|})(G \log G)\frac{N}{(\log(2 + rG/T^2))^3}$$

$$\ll \sum_{\substack{G,N \in \{2,4,8,\dots\} \\ GN \ll T}} T(\frac{T}{|GN|})^{0.1}(G \log G)\frac{N}{(\log G)^3} \ll T^2$$

for $3 \leq T \leq 2 + r^{1/2}$, by summing over N and then over G.

Final moments

We thus obtain the following result:

Theorem (W.–Xu 2024)

Suppose $\|q\theta\| := \min_{a\in\mathbb{Z}}|q\theta - a| \gg \exp(-q^{1/4})$ *for all* $q \in \mathbb{N}$.
If $x \ggg 1$, *then* $\mathbb{E}_{\chi \bmod r}|S(\chi,\theta;x)|^b \asymp x^{b/2}$ *for all* $0 \le b \le 4$.

Final moments

We thus obtain the following result:

Theorem (W.–Xu 2024)

Suppose $\|q\theta\| := \min_{a\in\mathbb{Z}}|q\theta - a| \gg \exp(-q^{1/4})$ *for all* $q \in \mathbb{N}$. *If* $x \ggg 1$, *then* $\mathbb{E}_{\chi \bmod r}|S(\chi,\theta;x)|^b \asymp x^{b/2}$ *for all* $0 \le b \le 4$.

(Setting of the theorem: Fix a smooth function $w\colon \mathbb{R} \to \mathbb{R}$, supported on $[0,1]$, with $\int_0^1 w(t)^2\,dt > 0$. Let

$$S(\chi,\theta;x) := \sum_{n\in\mathbb{Z}} \chi(n)e(n\theta)w(n/x) = \sum_{1\le n\le x} \chi(n)e(n\theta)w(n/x),$$

Fix $\theta \in \mathbb{R}$. Assume $1 \le x \le r$.)

Some interesting behavior

Shala used work of Matomäki (Diophantine approximation with prime denominators), the Burgess bound, and properties of Gauss sums, to prove the following result:

Theorem (Shala 2024)

There is a sequence of prime $r \to \infty$ such that the distribution of $\frac{1}{\sqrt{r}} \sum_{1 \le n \le r} \chi(n) e(n\sqrt{2})$ tends to the uniform distribution on the unit circle. (In particular, not Gaussian!)

(Thanks to Bober, Klurman, and Shala for informing us of this result.)

Comparison with [Heap–Sahay 2024]

Recently we learned of the following result, concerning the *periodic zeta function* (dual to the *Hurwitz zeta function*)

$$P(s,\theta) = \sum_{n\geq 1} \frac{e(n\theta)}{n^s},$$

which uses related Diophantine approximation techniques.

Theorem (Heap–Sahay 2024, in *Crelle* 2025)

Suppose $\|q\theta\| := \min_{a\in\mathbb{Z}}|q\theta - a| \gg 1/q^{2-\delta}$ *for all* $q \in \mathbb{N}$, *for some* $\delta > 0$.[a] *Then for* $0 \leq b \leq 4$ *and large* T, *we have*

$$\int_T^{2T} |P(\tfrac{1}{2} + it, \theta)|^b \asymp T(\log T)^{b/2}.$$

[a] Equivalently, the *irrationality measure* $\mu(\theta)$ of θ is < 3.

Comparison with [Heap–Sahay 2024]

Recently we learned of the following result, concerning the *periodic zeta function* (dual to the *Hurwitz zeta function*)

$$P(s,\theta) = \sum_{n\geq 1} \frac{e(n\theta)}{n^s},$$

which uses related Diophantine approximation techniques.

Theorem (Heap–Sahay 2024, in *Crelle* 2025)

Suppose $\|q\theta\| := \min_{a\in\mathbb{Z}}|q\theta - a| \gg 1/q^{2-\delta}$ *for all* $q \in \mathbb{N}$, *for some* $\delta > 0$.[a] *Then for* $0 \leq b \leq 4$ *and large* T, *we have*

$$\int_T^{2T} |P(\tfrac{1}{2} + it, \theta)|^b \asymp T(\log T)^{b/2}.$$

[a] Equivalently, the *irrationality measure* $\mu(\theta)$ of θ is < 3.

Can our methods be used to relax their Diophantine condition?