Families and dichotomies in the circle method

Victor Wang

Courant (NYU)

Stanford Student Analytic Number Theory Seminar, November 2022

Some motivation

Diophantine equations in the tradition of Hardy–Littlewood, and *L-functions* in the tradition of Riemann, are central objects in number theory. Some natural problems and questions about them are the following:

1. Count/produce/bound solutions to algebraic equations over the integers ($\mathbb{Z}$) or related rings (e.g. $\mathbb{F}_p[t]$ or $\mathbb{F}_p$).
2. Prove approximations to GRH[1] for individual L-functions, or analyze statistics (esp. those of Random Matrix Theory type) over families.
3. To what extent are (1)–(2) related?

[1] the Grand Riemann Hypothesis

Example (BSD)

Let $C/\mathbb{Q}$ be a smooth cubic curve in $\mathbb{P}^2$ with a $\mathbb{Q}$-point. (For example, $x^3 + y^3 + 60z^3 = 0$, but not $3x^3 + 4y^3 + 5z^3 = 0$.)

- The number of primitive integral solutions $(x, y, z) \ll X$ is $\alpha_C (\log X)^{r_C/2}$ as $X \to \infty$. Here $\alpha_C > 0$ and $r_C \in \mathbb{Z}_{\geq 0}$.
- Birch–Swinnerton-Dyer '65 conjectured that

$$r_C = \operatorname{ord}_{s=1/2} L(s, C),$$

where $L(s, C)$—the *Hasse–Weil L-function* associated to C—encodes the behavior of C mod p as prime p varies.

The "$\geq$" direction (local-to-global), i.e. "producing" points, remains especially mysterious.[2] But modularity (Wiles et al.) often helps, via Heegner points (Gross–Zagier '86).[3]

[2] But both directions are hard and interesting.

[3] Contrast with the use of modularity in Fermat's last theorem.

Example (Quadratic equations)

The most difficult part of the solution of Hilbert's eleventh problem (up to questions of effectiveness), namely the part regarding integral representations of integers by ternary quadratic forms with integral coefficients (due to Iwaniec, Duke, and Schulze-Pillot over $\mathbb{Q}$), also makes essential use of automorphic forms, through subconvex L-function bounds obtained through the study of L-function families.

Remark

Rational representations are much simpler, with a very clean existence theory (a local-to-global principle with no exceptions) given by Hasse–Minkowski, quantifiable by the sharpest forms of the circle method (e.g. the delta method, to be discussed).

Sums of 3 cubes (cf. BSD; but less structure?)

Mordell '53:

- Maybe producing large, general[4] integer solutions to

$$x^3 + y^3 + z^3 = a$$

  is as hard as "finding when an assigned sequence, e.g. 123456789, occurs in the decimal expansion of π"?
- Is there a solution for $a = 3$ after

$$3 = 1^3 + 1^3 + 1^3 = 4^3 + 4^3 + (-5)^3?$$

In general, if solutions exist, they are expected to be very rare.[5]

---

[4] say non-parametric

[5] Cf. Hypothesis K of Hardy–Littlewood '25 that $r_3(a) \leq C(\epsilon) a^{\epsilon}$ for $a \geq 1$; it is false, but certainly $\mathbb{E}_{1 \leq a \leq A}[r_3(a)] \sim C$.

The story of 33

Via computer, Booker obtained (at “five past nine in the morning on the 27th of February 2019”)

$$(8866128975287528)^3 + (-8778405442862239)^3 + (-2736111468807040)^3 = 33.$$

Later with Sutherland (September 2019):

$$(-80538738812075974)^3 + (80435758145817515)^3 + (12602123297335631)^3 = 42.$$

Also,

$$(569936821221962380720)^3 + (-569936821113563493509)^3 + (-472715493453327032)^3 = 3,$$

thus affirmatively answering a question of Mordell.

Main talk overview

Let $F(\boldsymbol{x}) := x_1^3 + \cdots + x_6^3$. This talk centers around Diophantine equations and L-functions, especially

1. $V : F(\boldsymbol{x}) = 0$ over $\mathbb{Z}$, as well as
2. $V_{\boldsymbol{c}} : F(\boldsymbol{x}) = \boldsymbol{c} \cdot \boldsymbol{x} = 0$ over $\mathbb{F}_p, \mathbb{Z}_p, \mathbb{R}$ (as $\boldsymbol{c}, p$ vary), and
3. the associated Hasse–Weil L-functions $L(s, V_{\boldsymbol{c}})$ (over $\Delta(\boldsymbol{c}) \neq 0$).

Problem (Many authors)

Estimate the number of integral solutions to $F(\boldsymbol{x}) = 0$ in expanding boxes or other regions.

Remark (Many authors)

This problem is closely tied to the statistics of *sums of* 3 *cubes*, via certain second moments (measuring the failure of injectivity of the map $(x, y, z) \mapsto x^3 + y^3 + z^3$).

Further motivation and context

A central theme in analytic number theory is *randomness*, appearing for instance in the following two questions:

1. Let H be a projective hypersurface over $\mathbb{Q}$. Does the "Hardy–Littlewood model" capture the behavior of $N_H(B)$ (the number of $\mathbb{Q}$-points on H of height $\leq B$) as $B \to \infty$?
2. Let X be a projective hypersurface over $\mathbb{F}_p$. Let

   $$E(X, \mathbb{F}_{p^r}) := \#X(\mathbb{F}_{p^r}) - \#\mathbb{P}^{\dim X}(\mathbb{F}_{p^r}).$$

   As $r \to \infty$, does $|E(X, \mathbb{F}_{p^r})| \ll (p^r)^{(\dim X)/2}$ (a naive generalization of GRH/$\mathbb{F}_p$) hold?

Often a *failure of randomness* can be explained by *structure*, e.g. special subvarieties, or Brauer–Manin obstructions, or (less satisfactorily) "logic" as in Hilbert's tenth problem...

Background on critical statistics (for $k \in \{2, 3\}$)

Let $r_k(a) := \#\{(x_1, \ldots, x_k) \in \mathbb{Z}_{\geq 0}^k : x_1^k + \cdots + x_k^k = a\}$ be the number of ways to write a as a sum of k integer kth powers.

1. Uniformly over $a \geq 1$, we have $r_2(a) \ll_\epsilon a^\epsilon$.
2. How about on average? In fact, $\sum_{a \leq X^2} r_2(a) \sim C_1 X^2$, and $\sum_{a \leq X^2} r_2(a)^2 \sim C_2 X^2 \log X$, as $X \to \infty$.[6]
3. For r_3, still have $\sum_{a \leq X^3} r_3(a) \sim C_3 X^3$ for first moment.[7]
4. *Conjecturally* (Hooley '86a): $\sum_{a \leq X^3} r_3(a)^2 \sim C_4 X^3$, and $> 0\%$ of integers are sums of 3 nonnegative cubes.[8]

Remark (Many authors)

$\sum_{a \leq X^3} r_3(a)^2 = \#\{\boldsymbol{x} \in \mathbb{Z}^6 \cap XK : x_1^3 + \cdots + x_6^3 = 0\}$ for some fixed compact region $K \subseteq \mathbb{R}^6$.

[6] Related: 0% of integers $a \geq 0$ are sums of 2 squares.

[7] But pointwise, $r_3(a) \gg a^{1/12}$ for infinitely many $a \geq 0$ (Mahler '36).

[8] In fact, the same holds for any positive-density subset of integer cubes.

As before, let $F(\boldsymbol{x}) = F(x_1, \ldots, x_6) := x_1^3 + \cdots + x_6^3$.

Definition

Let $N_{F,K}(X) := \#\{\boldsymbol{x} \in \mathbb{Z}^6 \cap XK : F(\boldsymbol{x}) = 0\}$, for K a nice[a] compact region in $\mathbb{R}^6$. (Or just use smooth weights!)

[a] Assume the boundary of K is suitably transverse to $F = 0$.

Definition

Hardy–Littlewood ("randomness model") prediction for $F = 0$:

$$N_{F,K}(X) \approx c_{\mathrm{HL}} \cdot X^{6-3}, \, ^{a}$$

where the constant $c_{\mathrm{HL}} := \sigma_{\mathbb{R}} \cdot \prod_p \sigma_p \in [0, \infty]$ is a product of local densities measuring the "local" (i.e. real and p-adic) bias of the equation $F = 0$ (over the regions $K \subseteq \mathbb{R}^6$ and $\mathbb{Z}_p^6$).

[a] the -3 indicating "how hard it is to satisfy a cubic equation"

Randomness and structure (for $F := x_1^3 + \cdots + x_6^3$)

Hooley '86a: HL ("randomness") prediction misses trivial solutions ("$x_i + x_j = 0$ in pairs"); maybe the truth is HLH?

Conjecture (HLH)

$N_{F,K}(X) = c_{\mathrm{HL}} \cdot X^3 + \#\{\text{trivial } \boldsymbol{x} \in \mathbb{Z}^6 \cap XK\} + o(X^3)$ holds as $X \to \infty$.

Remark (Around the square-root barrier)

1. The full HLH lies beyond the classical $\circ$-method (according to square-root "pointwise" minor arc considerations).
2. But the δ-method[a] opens the door to progress on HLH, by harmonically decomposing the true minor arc contribution in a "dual" fashion.

[a] Kloosterman '26, Duke–Friedlander–Iwaniec '93, Heath-Brown '96

What's known towards HLH?

1. Hua '38: $N_{F,K}(X) \ll X^{7/2+\epsilon}$ (by Cauchy b/w structure and randomness in $4, 8$ vars, resp.).
2. Vaughan '86+: $N_{F,K}(X) \ll X^{7/2}(\log X)^{\epsilon-5/2}$ (by new source of randomness).
3. Hooley '86+: $N_{F,K}(X) \ll X^{3+\epsilon}$, under "Hypothesis HW" ($\approx$ "modularity plus GRH") for the aforementioned Hasse–Weil L-functions $L(s, V_{\boldsymbol{c}})$.

Remark

1. Hooley used an "upper-bound precursor" to the δ-method.
2. The building blocks of the δ-method are certain Fourier transforms ("coefficients of wave decompositions").
   Which waves resonate throughout the frequency spectrum?
   Which components cancel out destructively?

Overview of Hooley's original approach

- Hooley's work uses the circle method (studying Fourier series in arcs $|\alpha - \frac{a}{q}| \le \frac{1}{qQ}$, for $q \le Q \asymp X^{3/2}$ and $a \perp q$), plus a clever use of an idea[9] of Kloosterman '26, to reduce the additive counting question $N_{F,K}(X) \le ?$ (about $F = 0$) to estimating a beautiful but complicated average over $\boldsymbol{c} \ll X^{1/2}$ of multiplicative quantities to moduli $q \le Q$.
- This led to the surprising appearance[10] of $1/L(s, V_{\boldsymbol{c}})$ over $\boldsymbol{c} \ll X^{1/2}$, which can be bounded for $\Re(s) > 1/2$ under standard NT hypotheses, e.g. modularity plus GRH.
- After a significant amount of work this leads (conditionally) to the near-optimal estimate $N_{F,K}(X) \ll_\epsilon X^{3+\epsilon}$. By my count, there are four or five different sources of epsilon!

[9] Poisson summation and averaging over a

[10] up to subtle algebro-geometric "error factors" related to a polynomial $\Delta(\boldsymbol{c})$ measuring the extent to which $V_{\boldsymbol{c}}$ is singular

The δ-method

Proposition (δ-method: Kloosterman '26, Duke–Friedlander–Iwaniec '93, Heath-Brown '96)

$$N_{F,K}(X) \approx\approx \mathbb{E}_{\boldsymbol{c} \ll X^{1/2}} \mathbb{E}_{n \le X^{3/2}} [n^{-1} S_{\boldsymbol{c}}(n)] =: \star$$

($\boldsymbol{c} \in \mathbb{Z}^6$), where $\approx\approx$ means I may be lying a bit, and

$$S_{\boldsymbol{c}}(n) := \sum_{1 \le a \le n : a \perp n} \sum_{1 \le x_1, \ldots, x_6 \le n} e^{2\pi i (aF(\boldsymbol{x}) + \boldsymbol{c} \cdot \boldsymbol{x})/n}.$$

Remark

The thresholds $X^{1/2}, X^{3/2}$ for $\boldsymbol{c}, n$ measure the "complexity of cubic problems" (a la Nyquist–Shannon). Here $\boldsymbol{c} = 0$ captures major arcs (roughly speaking), producing HL but not full HLH.

The $S_{\boldsymbol{c}}(n)$'s relate to $V_{\boldsymbol{c}} = \{[\boldsymbol{x}] \in \mathbb{P}^5 : F(\boldsymbol{x}) = \boldsymbol{c} \cdot \boldsymbol{x} = 0\}$.
Fact: $\exists$ disc poly $\Delta \in \mathbb{Z}[\boldsymbol{c}]$ measuring singularities of $V_{\boldsymbol{c}}$.

Lemma (Hooley)

If $\Delta(\boldsymbol{c}) \neq 0$, then $\widetilde{S}_{\boldsymbol{c}}(n) := n^{-7/2} S_{\boldsymbol{c}}(n)$ look (to 1st order) like the coeffs $\mu_{\boldsymbol{c}}(n)$ of $1/L(s, V_{\boldsymbol{c}})$.

Partial proof sketch.

Here F is homog (and a is summed), so $S_{\boldsymbol{c}}(n)$ is multiplicative.
Locally: If $p \nmid \boldsymbol{c}$, then $\widetilde{S}_{\boldsymbol{c}}(p) = \widetilde{E}_{\boldsymbol{c}}(p) + O(p^{-1/2})$, where
$\widetilde{E}_{\boldsymbol{c}}(p) := p^{-3/2}[\#V_{\boldsymbol{c}}(\mathbb{F}_p) - \#\mathbb{P}^3(\mathbb{F}_p)]$. Now use LTF. $\square$

Exercise (Cf. Hooley, "$\underline{\underline{2}}\times$-Kloosterman")

"Assume" $\forall \boldsymbol{c}, n, N$: $\Delta(\boldsymbol{c}) \neq 0$, $\widetilde{S}_{\boldsymbol{c}}(n) = \mu_{\boldsymbol{c}}(n)$,
$\sum_{n \leq N} \mu_{\boldsymbol{c}}(n) \ll \|\boldsymbol{c}\|^{\epsilon} N^{1/2+\epsilon}$. Then $\star \ll X^{3+\epsilon}$.

Theorem (Hooley '86+/Heath-Brown '98)

$N_{F,K}(X) \ll_\epsilon X^{3+\epsilon}$, under Hypo HW ($\approx$ modularity + GRH) for $L(s, V_{\boldsymbol{c}})$'s (over $\Delta(\boldsymbol{c}) \neq 0$).[a]

[a] A large-sieve hypo would suffice (W.). It's open! But $\exists$ uncond. apps to $x^2 + y^3 + z^3$ (W., via Brüdern '91 + Duke–Kowalski '00 + Wiles et al).

There are several critical sources of ϵ in Hooley/Heath-Brown, including the locus $\Delta(\boldsymbol{c}) = 0$ we have not yet discussed.

Theorem (W. '21; unconditional)

The main terms of HLH come from the locus $\Delta(\boldsymbol{c}) = 0$.

Proof hint.

We shall soon see why this is plausible (failure of "naive generalization" of GRH/$\mathbb{F}_p$ caused by special subvarieties). $\square$

An optimal dichotomy over finite fields

Theorem (W. '22)

The following are equivalent for a cubic threefold X of the form $x_1^3 + \cdots + x_6^3 = c_1x_1 + \cdots + c_6x_6 = 0$ over $\mathbb{F}_p$ for $p \gg 1$:[a]

1. *X fails the "naive generalization" of GRH/$\mathbb{F}_p$.*
2. *$X_{\overline{\mathbb{F}}_p}$ contains a plane.*
3. *$X_{\overline{\mathbb{F}}_p}$ contains a plane lying on the Fermat cubic fourfold $x_1^3 + \cdots + x_6^3 = 0$.*
4. *$X_{\overline{\mathbb{F}}_p}$ contains $x_1 + x_2 = x_3 + x_4 = x_5 + x_6 = 0$ (up to Fermat symmetries).*
5. *$c_1^3 - c_2^3 = c_3^3 - c_4^3 = c_5^3 - c_6^3 = 0$ (up to symmetry).*

---

[a] These hyperplane sections arise naturally in the context of the Fourier transforms $S_{\boldsymbol{c}}(p) = \sum_{1 \le a \le p-1} \sum_{1 \le x_1, \ldots, x_6 \le p} e^{2\pi i (a(x_1^3 + \cdots + x_6^3) + \boldsymbol{c} \cdot \boldsymbol{x})/p}$.

The previous dichotomy follows from the following subtler, more general dichotomy.[11]

Theorem (W. '22)

For a cubic threefold $X \subseteq \mathbb{P}^4_{\mathbb{F}_p}$ of the form $C(x_1, \dots, x_5) = 0$ with at most isolated singularities, the following are equivalent:

1. *X fails the "naive generalization" of GRH/$\mathbb{F}_p$.*
2. *There exist quadratic forms $Q_1, Q_2 \in \overline{\mathbb{F}}_p[x_1, \dots, x_5]$ "essentially in 4 variables",[a] and a homogeneous polynomial $A \in \overline{\mathbb{F}}_p[x_1, \dots, x_5]$, such that $A \cdot C \in (Q_1, Q_2)$ and $A \notin \sqrt{(Q_1, Q_2)}$.*[b]
3. *$X_{\overline{\mathbb{F}}_p}$ contains a plane or a singular cubic scroll.*

[a] i.e. Q_1, Q_2 with a common nonzero singularity

[b] I think it might be possible to take $\deg A \leq 1$, but have not checked.

[11] Reduction: A calculation—a singularity analysis—involving, among other things, 3×3 Vandermonde determinants arising from diagonality.

Remark

The proof of the "more general dichotomy" combines classical geometry (including work of del Pezzo et al.), on the one hand, with amplificatory base change via modern geometry (Katz, Skorobogatov, et al.), on the other.

I like the statement[12] more than the proof (which relies on some not-very-robust situation-specific geometry).

Question

Is there a more enlightening or more general proof? Can one avoid or minimize use of base change? Can one use auxiliary polynomials or other tools?

[12] which, to me, is suggestive as to what may be true more generally

The significance of the threefold dichotomy is threefold:

1. It gives an explicit "codimension 3" bound on the "locus of failures" of the "naive generalization" of $\mathrm{GRH}/\mathbb{F}_p$.
   - One can also (Lindner '20 + Lefschetz pencil theory) give an explicit "codimension 2" bound in terms of iterated discriminants (cf. Bhargava '22).
   - Or (probably; cf. Grimmelt–Sawin '21) an inexplicit "codimension 2" bound via perversity machinery of Fouvry–Katz '01 for Fourier transforms.
2. The dichotomy implies that special subvarieties in HLH/Manin for the cubic fourfold $x_1^3 + \cdots + x_6^3 = 0$ "remain special" for hyperplane sections modulo p.
   - On $x_1^4 + x_2^4 + x_3^4 = x_4^4 + x_5^4 + x_6^4$, does a similar story hold for (Wooley's favorite special subvariety?)

     $$x_1+x_2+x_3 = x_4+x_5+x_6 = (x_1^2+x_2^2+x_3^2)-(x_4^2+x_5^2+x_6^2) = 0?$$
3. It can prove some consequences of Deligne–Katz equidistribution involved in RMT-type prediction recipes.

The p-adic ladder

Besides $S_{\boldsymbol{c}}(p)$, there are other Fourier transforms of interest:

$$S_{\boldsymbol{c}}(p^l) = \sum_{1 \le a \le p^l : p \nmid a} \sum_{1 \le x_1, \ldots, x_6 \le p^l} e^{2\pi i (a(x_1^3 + \cdots + x_6^3) + \boldsymbol{c} \cdot \boldsymbol{x})/p^l},$$

for $l \ge 2$. We bound these using various partial analogs[13] of the following results for univariate polynomials. Given $f \in \mathbb{Z}[x]$ and an integer $q \ge 1$, let $N(f; q) := \#\{x \in \mathbb{Z}/q\mathbb{Z} : f(x) = 0\}$.

- Sándor '52: If p is a prime and $l \ge 2 + v_p(\operatorname{disc} f)$, then $N(f; p^l) - p^0 N(f; p^{l-1}) = 0$ (stabilization occurs).
- Huxley '81: If p is a prime and $l \ge 1$, then

$$N(f, p^l) \le (\deg f) \cdot p^{v_p(\operatorname{disc} f)/2}$$

(a stratified bound in terms of how much p divides $\operatorname{disc} f$).

[13] some new, some old

A consequence

The dichotomy and ladder provide *discriminating pointwise estimates* on $S_{\boldsymbol{c}}(n)$. Together with *general pointwise estimates* of Hooley and Heath-Brown, these let us reduce a useful statement, (B3), to a standard hypothesis, (SFSC).

Conjecture (B3, roughly; "cf. Sarnak–Xue")

For some $\delta > 0$: Over $\boldsymbol{c} \in [-Z, Z]^6$ with $\Delta(\boldsymbol{c}) \neq 0$, the probability there exists an integer $n \leq Z^3$ such that $|S_{\boldsymbol{c}}(n)|$ fails square-root cancellation by a factor of $\geq \lambda \cdot n^{1/2-\delta}$ is $O(\lambda^{-2})$.

Conjecture (SFSC, roughly)

Over $\boldsymbol{c} \in [-Z, Z]^6$ with $\Delta(\boldsymbol{c}) \neq 0$, the probability there exists a prime $p \geq P$ with $p^2 \mid \Delta(\boldsymbol{c})$ is $O(P^{-\delta})$, for some $\delta > 0$.

(B3) would *fail* if we replaced $x_1^3 + \cdots + x_6^3$ with $x_1^2 + \cdots + x_6^2$.

Theorem (W. '21; conditional)

Roughly: Under RMT-type predictions[a] *and (B3), the locus* $\Delta(\boldsymbol{c}) \neq 0$ *in the* δ*-method contributes* $O(X^3)$*; in fact,* $o(X^3)$*.*

[a] We use the Ratios Conjectures of Conrey–Farmer–Zirnbauer '08.

Proof hint.

Appropriately decompose $S_{\boldsymbol{c}}(n)$ to isolate distinct[a] behaviors.[b] For $O(X^3)$, use Hölder appropriately between "good" and "bad" factors; some important ingredients are (B3) and (R2').
For $o(X^3)$, handle some ranges (namely those with large "error moduli") the same. Over what remains, decompose $\Sigma_{\Delta \neq 0}$ into "error-constant" pieces—based on Δ—up to a small exceptional set constructed by algorithmic tree-like means. Then estimate these pieces via local calculations and Poisson summation. $\square$

[a] distinct at least under current philosophy

[b] Roughly: "L-approximations", "good errors", and "bad factors".

A sample RMT-type ingredient

Over $\Delta(\boldsymbol{c}) \neq 0$, the reciprocal L-functions $1/L(s, V_{\boldsymbol{c}})$ are the main players. The Ratios Conjectures imply e.g. the following:

Conjecture (R2', roughly)

Let $\sigma > 1/2$ and $1 \leq N \leq X^{3/2}$. If $s = \sigma + it$, then

$$\mathbb{E}_{\substack{\boldsymbol{c} \ll X^{1/2}: \\ \Delta(\boldsymbol{c}) \neq 0}} \left| \int_{\mathbb{R}} dt\, e^{s^2} N^s \cdot \frac{\zeta(2s)^{-1} L(s+1/2, V)^{-1}}{L(s, V_{\boldsymbol{c}})} \right|^2 \ll N.$$

- The LHS is independent of σ.[14]
- There are no $\log N$ or $\log X$ factors on the RHS![15]
- This is enough "RMT input" for $N_{F,K}(X) \ll X^3$.

[14] One could take $\sigma - \frac{1}{2} \asymp \frac{1}{\log X}$ to facilitate comparison with other work.

[15] At least up to mollification/integration, logs reflect "symmetry type" of a family. Our L-functions are expected to behave like the characteristic polynomials of $C \times C$ random orthogonal matrices with $C \ll \log X$.

Remark

- Up to Cauchy–Schwarz over s (losing $\log X$?), (R2') might be very similar to well-studied moments (cf. Sound '09 and Harper '13 on moments of zeta, and Bui–Florea–Keating '21 and Florea '21 on negative moments of L-functions).
- But because the integral is inside in the absolute value, (R2') is really a statement about log-free cancellation over $n \asymp N$ of the coefficients of $\frac{\zeta(2s)^{-1} L(s+1/2, V)^{-1}}{L(s, V_c)}$. This resembles the (unconditional!) log-free bound

$$\frac{1}{X} \sum_{\substack{m \asymp X: \\ \mu(m)^2 = 1}} \left| \sum_{n \asymp X} \tilde{\lambda}_f(n) \left(\frac{m}{n}\right) \right|^2 \ll X$$

of Xiannan Li regarding certain orthogonal families of quadratic twists (see (1.3) of arXiv:2208.07343v2).

More on mean values (Cancellation over $\boldsymbol{c}$)

The Ratios Conjectures also predict the following for $\sigma > 1/2$:[16]

Conjecture (R1, roughly)

Write $s = \sigma + it$. For some $\delta > 0$ (independent of σ),

$$\mathbb{E}_{\substack{\boldsymbol{c} \ll X^{1/2}: \\ \Delta(\boldsymbol{c}) \neq 0}} \left[\frac{1}{L(s, V_{\boldsymbol{c}})} - \underbrace{\zeta(2s) L(s + 1/2, V)}_{\text{polar factors}} A_F(s) \right] \ll_{\sigma,t} X^{-\delta}$$

for $X \geq 1$. Here $A_F(s) \ll 1$ for $\Re(s) \geq 1/2 - \delta$.

Remark

For $N_{F,K}(X) \ll X^3$, we only use (R2'). But for HLH, we need a "slight adelic perturbation" (RA1) of (R1).

[16] A soft asymptotic for $\sigma - \frac{1}{2} \asymp \frac{1}{\log X}$ should also suffice for soft HLH.

Main result

Theorem (W. '21)

Roughly: Assume standard NT hypotheses on L-functions and "unlikely" divisors. Then $N_{F,K}(X) \ll X^3$*, and in fact HLH Conj. holds for a large class of regions* K*. (Actual hypo's for former are cleaner than those for latter.)*

More precisely, hypotheses are the following:

- $L(s, V_{\boldsymbol{c}}), L(s, V_{\boldsymbol{c}}, \bigwedge^2), L(s, V)$ (Hypo HW2 + Ratios Conj's, where (R2') suffices for $N_{F,K}(X) \ll X^3$),
- Square-free Sieve Conjecture for $\Delta(\boldsymbol{c})$, and
- "effective Krasner"[17] if one wants a power saving in HLH.

These are all essentially hypotheses about the family of Hasse–Weil L-functions $L(s, V_{\boldsymbol{c}})$ over $\boldsymbol{c} \ll X^{1/2}$.

[17] "effective version of Kisin's thesis"

Glossary for hypo's

1. Hypo HW2: Similar in spirit to Hooley's Hypo HW.
2. Ratios Conj's: Give predictions of Random Matrix Theory (RMT) type for mean values of $1/L(s, V_{\boldsymbol{c}})$ and $1/L(s_1, V_{\boldsymbol{c}})L(s_2, V_{\boldsymbol{c}})$ over families of $\boldsymbol{c}$'s.[18]
3. "Effective Krasner": Need $L_p(s, V_{\boldsymbol{c}})$ to only depend on $\boldsymbol{c}$ mod $p\Delta(\boldsymbol{c})^{1000}$ (cf. Kisin's thesis, *Local constancy in p-adic families of Galois representations*).
4. SFSC: Need, for $Z \geq 1$ and $P \leq Z^{3/2}$, an upper bound of $O(Z^6 P^{-\delta})$ for

$$\#\{\boldsymbol{c} \in [-Z, Z]^6 : \exists\, p \in [P, 2P] \text{ with } p^2 \mid \Delta(\boldsymbol{c})\}.$$

[18] Conrey–Farmer–Zirnbauer '08 build on other historical works, such as Conrey–Farmer–Keating–Rubinstein–Snaith '05, which in turn build on predictions for L-zeros "in the bulk" of Montgomery–Dyson '70s and others, and "near 1/2" of Katz–Sarnak '90s.

Application to representing integers and primes

Theorem (W. '21, roughly)

Assume the same hypotheses as before. Then $N_{F,K}(X) \ll X^3$ *for a large class of regions* K*. In fact, one gets an asymptotic featuring a randomness-structure dichotomy.*[a] *Consequently,* 100% *of integers* $a \not\equiv \pm 4 \bmod 9$ *are sums of three cubes.*[b]

[a] cf. conjectures of Hooley, Manin, Vaughan–Wooley, Peyre, et al.
[b] This follows from "HLH for sufficiently many K" (Diaconu '19 + ϵ).

Theorem (W. '22, roughly)

Assume roughly the same hypotheses as above. Then 100% *of primes* $p \not\equiv \pm 4 \bmod 9$ *are sums of three cubes.*[a]

[a] This follows from "HLH with a power saving for sufficiently many K, with small divisibility constraints $d \mid x_1^3 + x_2^3 + x_3^3, x_4^3 + x_5^3 + x_6^3$".

Approach to primes

To capture primes one can apply the Selberg sieve to a certain "approximate variance" for sums of three cubes. What would the Selberg sieve give towards the following question?

Question

Assuming precise asymptotic second moments for $r_3(a)$ over $\{a \leq A : a \equiv 0 \bmod d\}$ for $d \leq A^\delta$,[a] can one show for $A \geq 2$

$$\sum_{p \leq A} r_3(p)^2 \ll A/\log A?$$

[a] The expected main term for these second moments may not vary multiplicatively with d. This may or may not be a serious obstacle.

Here $r_3(a) := \#\{(x, y, z) \in \mathbb{Z}^3_{\geq 0} : x^3 + y^3 + z^3 = a\}$.
(The Selberg sieve does easily give $\sum_{p \leq A} r_3(p) \ll A/\log A$.)

Questions to explore

- Prove (R2'), at least up to logs, under GRH? Cf. Sound '09, Harper '13, Bui–Florea–Keating '21, and Florea '21.
- Function-field analogs (GRH is known; exist monodromy groups; but only know limited ranges of RMT conjectures).
- Understand the "subtle AG error factors" better; try to handle some non-diagonal analogs of $x_1^3 + \cdots + x_6^3 = 0$?
- $xyz = uvw$: NT basically understood ("multiplicative" harmonic analysis). Here can one go from NT to RMT?
- Hypothesis K (sparsity) fails for $x^3 + y^3 + z^3 = a$. What about Hypothesis K for $x^4 + y^4 + z^4 + w^4 = a$? Lots of AG questions in this vein.
- Counting on quartics or other varieties: Try to combine symmetry (dynamical ideas?) and the circle method? Already exist many works using only one or the other.