Randomness and structure for sums of cubes

Victor Wang

Princeton University
Advised by Peter Sarnak

SNU Number Theory Seminar, April 2022

Some motivation

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

1. Let V be a projective hypersurface over $\mathbb{Q}$. Does the "Hardy–Littlewood model" capture the behavior of $N_V(B)$ (the number of $\mathbb{Q}$-points on V of height $\leq B$) as $B \to \infty$?
2. Let X be a projective hypersurface over $\mathbb{F}_p$. Let
$$E(X_{p^r}) := \#X(\mathbb{F}_{p^r}) - \#\mathbb{P}^{\dim X}(\mathbb{F}_{p^r}).$$
As $r \to \infty$, does a "square-root cancellation" bound, i.e. $|E(X_{p^r})| \ll (p^r)^{(\dim X)/2}$, 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...

Further motivation

Diophantine equations[1] and L-functions[2] 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[3] 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] in the tradition of e.g. Hardy–Littlewood

[2] in the tradition of e.g. Riemann

[3] 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, $x_1^3 + x_2^3 + 60x_3^3 = 0$, but not $3x_1^3 + 4x_2^3 + 5x_3^3 = 0$.) Then Birch–Swinnerton-Dyer '65 conjectured

$$\operatorname{rank} J(C)(\mathbb{Q}) = \operatorname{ord}_{s=1/2} L(s, C)$$

(an equality of integers), where

1. $\operatorname{rank} J(C)(\mathbb{Q})$ measures how many integral solutions $\boldsymbol{x} = (x_1, x_2, x_3) \in [-X, X]^3$ there are as $X \to \infty$, while
2. $L(s, C)$—the *Hasse–Weil L-function* associated to C—encodes the behavior of C mod p as p varies.

In general, the "$\geq$" direction, i.e. "producing" points, remains especially mysterious. But modularity (Wiles et al.) often helps, via Heegner points (Gross–Zagier '86).[a]

[a] 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).

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. $F(\boldsymbol{x}) = 0$ over $\mathbb{Z}$, as well as
2. $F(\boldsymbol{x}) = \boldsymbol{c} \cdot \boldsymbol{x} = 0$ over $\mathbb{F}_p$ (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*.

The usual randomness heuristic (via level sets)

Let $s := 6$. For $K \subset \mathbb{R}^s$ nice (cpt, semi-alg), $X \to \infty$, and $a \in \mathbb{Z}$, let $N_{F-a,K}(X) := \#\{\boldsymbol{x} \in \mathbb{Z}^s \cap XK : F = a\}$.

Example

Say $K = [-1,1]^s$. Then $XK = [-X,X]^s$, and

$$F(\mathbb{Z}^s \cap XK) \ll X^3 \quad \text{(since } F = x_1^3 + \cdots + x_s^3 \text{ is cubic).}$$

So $N_{F-a,K}(X)$ is $\asymp X^{s-3}$ *on avg* (in ℓ^1) over $a \ll X^3$.

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

$$N_{F,K}(X) \approx X^{s-3} \prod_{v \leq \infty} \sigma_v.$$

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

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

Conjecture (HLH)

For any nice $K \subset \mathbb{R}^6$,

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

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 opens the door to progress on HLH, by harmonically decomposing the true minor arc contribution in a "dual" fashion.

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+: " " $\ll X^{7/2}(\log X)^{\epsilon-5/2}$ (by new source of randomness).
3. Hooley '86+: " " $\ll X^{3+\epsilon}$, under Hypo HW ($\approx$ modularity $+$ GRH for the Hasse–Weil L-functions $L(s, V_{\boldsymbol{c}})$).

Hooley used an "upper-bound precursor" to the δ-method.

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

$$S_{\boldsymbol{c}}(n) := \sideset{}{'}\sum_{a \bmod n} \sum_{\boldsymbol{x} \in (\mathbb{Z}/n)^6} e_n(aF(\boldsymbol{x}) + \boldsymbol{c} \cdot \boldsymbol{x}).$$

($e_n(t) := e^{2\pi i t/n}$) (Don't worry about the "$'$"; it means $a \perp n$)

Remark

Here $\boldsymbol{c} = 0$ captures major arcs (roughly speaking), producing HL but not full HLH. And $\boldsymbol{c} \neq 0$ captures...

"Pf".

Idea ("Kloosterman method") is to treat classical major and minor arcs uniformly (using Poisson summation[a]), and average over a mod n.

$$N_{F,K}(X) \approx\approx \sum_{n \le X^{3/2}} \frac{1}{nX^{3/2}} \sum_{a \bmod n}' \sum_{\boldsymbol{x} \ll X} e_n(aF(\boldsymbol{x})) \quad (\circ\text{-method})$$

$$\approx\approx \sum_{n \le X^{3/2}} \frac{1}{nX^{3/2}} \mathbb{E}_{\boldsymbol{c} \ll n/X}[S_{\boldsymbol{c}}(n)] \quad (\text{“complexity” } n/X)$$

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

Idea': In gen'l (for $n \gg X$ large), $\sum'_{a \bmod n} \sum_{\boldsymbol{x} \ll X} e_n(aF(\boldsymbol{x}))$ is incomplete mod n, but still a wt'd avg of the complete sums $S_{\boldsymbol{c}}(n)$, if we sample over enough $\boldsymbol{c}$'s (Nyquist–Shannon). □

[a] with $\boldsymbol{c} = 0$ "purely probabilistic", and $\boldsymbol{c} \neq 0$ subtler

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

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 $1/L(s, V_{\boldsymbol{c}})$ ($V_{\boldsymbol{c}} := (\mathcal{V}_{\boldsymbol{c}})_{\mathbb{Q}}$).

Partial proof sketch.

Here F is homog (& 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 $\widetilde{E}_{\boldsymbol{c}}(p) := p^{-3/2}[\#\mathcal{V}_{\boldsymbol{c}}(\mathbb{F}_p) - \#\mathbb{P}^3(\mathbb{F}_p)]$. 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 $\star \ll X^{3+\epsilon}$.

By coincidence, the "double Kloosterman" misses HLH by ϵ.

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).

Theorem (W.)

Roughly: Assume standard NT conjectures on L-functions (e.g. Hypo HW + RMT-type predictions) and "unlikely" divisors ("$p^2 \mid \Delta(\boldsymbol{c})$").
Then $N_{F,K}(X) \ll X^3$, and in fact HLH Conj. holds for a large class of regions K.[a]

[a] This has nice applications to sums of 3 cubes (Diaconu '19 + ϵ).

More precisely:

Theorem (W.)

Assume standard NT conj's on

- $L(s, V_{\boldsymbol{c}}), L(s, V_{\boldsymbol{c}}, \bigwedge^2), L(s, V(F))$ *(Hypo HW2 + Ratios Conj's + Krasner*[a]*), and*
- *"unlikely" divisors (Square-free Sieve Conjecture for* $\Delta(\boldsymbol{c})$*).*

Then for any nice $K \subset \mathbb{R}^6$ *w/* $K \cap \operatorname{hess} F = \emptyset$*,*[b] *we have* $N_{F,K}(X) \ll X^3$*, & in fact HLH Conj. holds. (Actual hypo's for former are cleaner than those for latter.)*

---

[a] "effective version of Kisin's thesis (*Local constancy in p-adic families of Galois representations*)"

[b] This could probably be removed with enough work, but is mild enough for our main qualitative needs.

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.[4]
3. Krasner: Need $L_p(s, V_{\boldsymbol{c}})$ to only depend on $\boldsymbol{c}$ mod $p\Delta(\boldsymbol{c})^{1000}$ (cf. Kisin's thesis).
4. SFSC: Need (for $Z \geq 1$, $P \leq Z^3$)

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

[4] How does $\boldsymbol{c} \mapsto L(s, V_{\boldsymbol{c}})$ behave on average? RMT predictions originated for L-zeros "in the bulk" from Montgomery–Dyson, and "near 1/2" from Katz–Sarnak. CFKRS (2005) developed *full main term* predictions for L-powers, and CFZ (2008) for L-ratios.

Proof hint.

We want to bound/estimate (via δ-method)

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

Exponent numerics over various loci (if $d = 3$, $s = 6$):

$$\underbrace{s - d}_{\boldsymbol{c}=0,\ n \text{ small}} = \underbrace{\frac{s}{2} + \cancel{O(\epsilon)}}_{\Delta(\boldsymbol{c})=0,\ n \text{ large}} = \underbrace{\frac{d}{4}(s - \underline{\underline{2}}) + \cancel{O(4\epsilon)}}_{\Delta(\boldsymbol{c})\neq 0}$$
$$= 3 + \cancel{O(5\epsilon)}.$$

Main terms of HLH: $\Delta(\boldsymbol{c}) = 0$ (key: $S_{\boldsymbol{c}}(n)$ is biased for special $\boldsymbol{c}$'s). Conditional/hardest part: $\Delta(\boldsymbol{c}) \neq 0$ (which "factors" into certain mean-value and pointwise estimates over $\boldsymbol{c}$). □

Remark (Some more details)

There are maybe 5 sources of ϵ in Hooley/Heath-Brown, incl. what I'll call "Special", "Generic", & "Bad$p$".
The locus $\Delta(\boldsymbol{c}) = 0$ in $\star$ *unconditionally* produces the conj'd main term $c_{\mathrm{HLH}} \cdot X^3$. This resolves "Special".
The remaining sum (over $\Delta(\boldsymbol{c}) \neq 0$) is *conditionally*

$$\approx\approx \sum_{\text{finite set}} (\text{typically } O(1))^{a} \times (\text{RMT-type sum}).$$

- To prove "typical-$O(1)$" (*under* SFSC), re: "Bad$p$", need partial results towards a dichotomy/$\mathbb{F}_p$.
- Each "RMT-type sum" is $0 + O(X^{3-\delta})$ (*under* Ratios), improving on GRH bound $O_\epsilon(X^{3+\epsilon})$ (cf. "Generic").

[a] needs proof; loosely resembles Sarnak–Xue "density philosophy"

A sample pointwise ingredient

We also use partial results[5] toward a dichotomy/$\mathbb{F}_p$, amusingly parallel to HLH:

Theorem (W. '22)

If p is sufficiently large, and $\boldsymbol{c} \in \mathbb{F}_p^6$ satisfies $|\#\mathcal{V}_{\boldsymbol{c}}(\mathbb{F}_p) - \#\mathbb{P}^3(\mathbb{F}_p)| \geq 10^{10} p^{3/2}$ ("randomness fails"), then $\mathcal{V}_{\boldsymbol{c}} \bmod p$ contains a plane (i.e. $c_i^3 = c_j^3$ in pairs; "some special structure holds"). This is part of a subtler general dichotomy.

Recall: $\mathcal{V}_{\boldsymbol{c}}$ is the hyperplane section $F(\boldsymbol{x}) = \boldsymbol{c} \cdot \boldsymbol{x} = 0$.
For large p, the planes on $\mathcal{V}$ (the zero locus of $F(\boldsymbol{x}) = x_1^3 + \cdots + x_6^3$ in $\mathbb{P}^5$) are cut out by "$x_i^3 + x_j^3 = 0$ in pairs" (e.g. $x_1 + x_2 = x_3 + x_4 = x_5 + x_6 = 0$).

[5] proven using "worst-case" results of Skorobogatov '92 (or Katz '91) and "average-case" results of Lindner '20

A sample mean-value 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)

For certain holomorphic $f(s)$, e.g. e^{s^2}, we have

$$\mathbb{E}'_{\boldsymbol{c} \ll X^{1/2}} \left| \int_{(\sigma)} ds \, \frac{\zeta(2s)^{-1} L(s+1/2, V(F))^{-1}}{L(s, V_{\boldsymbol{c}})} \cdot f(s) N^s \right|^2 \ll_f N$$

($\sigma > 1/2$; $1 \ll N \ll X^{3/2}$).

- There are no $\log N$ or $\log X$ factors on the RHS! Such factors are determined by the "symmetry type" of the underlying family of L-functions.
- This is enough "RMT input" for $N_{F,K}(X) \ll X^3$.

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

Also, for some $\delta > 0$, one expects the following:

Conjecture (R1, roughly)

$$\mathbb{E}'_{\boldsymbol{c} \ll X^{1/2}} \left[\frac{1}{L(s, V_{\boldsymbol{c}})} - \underbrace{\zeta(2s) L(s+1/2, V(F))}_{\text{polar factors}} A_F(s) \right] \ll_{\sigma,t} X^{-\delta}$$

(over $\Delta(\boldsymbol{c}) \neq 0$) (for $X \geq 1$; $s = \sigma + it$; $\sigma > 1/2$)
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 (which requires "cancellation over $\boldsymbol{c}$"), we need a "slight adelic perturbation" of (R1).

Applications to sums of 3 cubes

Let $g := x^3 + y^3 + z^3$.

Question (Integral Hasse principle)

Is every *admissible*[a] integer a represented by g (over $\mathbb{Z}$)?

[a] i.e. locally represented; i.e. $\not\equiv \pm 4 \bmod 9$

Theorem (S. Diaconu '19 + ϵ)

Say, $\forall$ nice $K \subset \mathbb{R}^6$, HLH holds. Then 100% *Hasse holds.*

Theorem (W.)

Assume standard NT conj's on L-functions (e.g. Hypo HW + "RMT") & "unlikely" divisors ("$p^2 \mid \Delta(\boldsymbol{c})$"). Then 100% *(resp. $>$* 0%*) of admiss. ints lie in* $g(\mathbb{Z}^3)$ *(resp.* $g(\mathbb{Z}^3_{>0})$*).*

The story of 33

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

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

Remark

See the Youtube video "33 and all that" for a nice talk by Booker (with T-shirt and mug links) on the discovery of this and related results.

Exercise

Try Google Calculator, then Wolfram Alpha.