Sums of cubes and Random Matrix Theory

Victor Wang

Courant (NYU)

Postdoc Seminar Day, November 2022

Some motivation (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 $3x^3 + 4y^3 + 5z^3 = 0$.) Then Birch–Swinnerton-Dyer '65 conjectured

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

(an equality of integers), where

1. $(\log X)^{r_C/2}$ is roughly how many primitive integral solutions $(x, y, z) \in [-X, X]^3$ 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 prime p varies.

The "$\geq$" direction (local-to-global), i.e. "producing" points, remains especially mysterious. But modularity (Wiles et al.) often helps, via Heegner points (Gross–Zagier '86).[1]

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

Sums of 3 cubes (harder?)

Mordell '53:

- Maybe producing large, general[2] 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 sparse. (Cf. Hypothesis K of Hardy–Littlewood '25 that $r_3(a) \leq C(\epsilon)a^\epsilon$ for $a \geq 1$; this is false, but certainly $\mathbb{E}_{1 \leq a \leq A}[r_3(a)] \sim C$.)

[2] say non-parametric

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):

$$(-8053873881207597 4)^3 + (8043575814581751 5)^3 + (1260212329733563 1)^3 = 42.$$

Also,

$$(5699368212219623807 20)^3 + (-5699368211135634935 09)^3 + (-4727154934533270 32)^3 = 3,$$

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 $(x, y, z) \mapsto x^3 + y^3 + z^3$).

Definition

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 like $[-1, 1]^6$.

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

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 standard NT hypotheses for the Hasse–Weil L-functions $L(s, V_{\boldsymbol{c}})$.

The circle method

- Hooley's work uses the circle method (studying Fourier series in arcs $|\alpha - \frac{a}{q}| \leq \frac{1}{qQ}$, for $q \leq Q \asymp X^{3/2}$ and $a \perp q$), plus a clever use of an idea[3] of Kloosterman '26, to reduce the additive counting question $N_{F,K}(X) =?$ (about $F = 0$) to estimating a beautiful but complicated average over $\boldsymbol{c} \ll X^{1/2}$ of multiplicative quantities to moduli $q \leq Q$.
- This led to the surprising appearance[4] 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!

---

[3] Poisson summation and averaging over a

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

Some thesis/recent work

Theorem (W. '21, roughly)

Assume, mainly, predictions of Random Matrix Theory (RMT) type for $1/L(s, V_{\boldsymbol{c}})$, *as* $\boldsymbol{c} \ll X^{1/2}$ *varies.*[a] *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.*[b] *Consequently,* 100% *of integers* $a \not\equiv \pm 4 \bmod 9$ *are sums of three cubes.*

---

[a] We use Conrey–Farmer–Keating–Rubinstein–Snaith '05 and Conrey–Farmer–Zirnbauer '08, which build on predictions for L-zeros "in the bulk" of Montgomery–Dyson '70s, and "near $1/2$" of Katz–Sarnak '90s.

[b] cf. conjectures of Hooley, Manin, Vaughan–Wooley, Peyre, et al.

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 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

$$\mathbb{E}'_{\boldsymbol{c} \ll X^{1/2}} \left| \int_{[-1,1]} dt\, N^s \cdot \frac{\zeta(2s)^{-1} L(s+1/2, V)^{-1}}{L(s, V_{\boldsymbol{c}})} \right|^2 \ll N.$$

- 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. Our L-functions are expected to behave like the characteristic polynomials of $C \times C$ random orthogonal matrices with $C \ll \log X$.
- This is enough "RMT input" for $N_{F,K}(X) \ll X^3$.

Questions to explore

- Prove (R2'), at least up to logs, under GRH? Cf. Sound, Harper on moments of zeta.
- 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.

Further motivation and details

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

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

   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...

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 $S_{\boldsymbol{c}}(p) := \sum_{a \in (\mathbb{Z}/p)^\times} \sum_{\boldsymbol{x} \in (\mathbb{Z}/p)^6} e^{2\pi i (a(x_1^3 + \cdots + x_6^3) + \boldsymbol{c} \cdot \boldsymbol{x})/p}$.

The previous dichotomy follows from a subtler, more general dichotomy involving special lower-degree polynomials (quadratics), or equivalently both planes and cubic scrolls.

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[5] 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?

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

The p-adic ladder

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

$$S_{\boldsymbol{c}}(p^l) := \sum_{a \in (\mathbb{Z}/p^l)^\times} \sum_{\boldsymbol{x} \in (\mathbb{Z}/p^l)^6} e^{2\pi i (a(x_1^3 + \cdots + x_6^3) + \boldsymbol{c} \cdot \boldsymbol{x})/p^l},$$

for $l \geq 2$. We bound these using various partial analogs[6] of the following results for univariate polynomials. Given $f \in \mathbb{Z}[x]$ and an integer $q \geq 1$, let $N(f; q) := \#\{x \in \mathbb{Z}/q\mathbb{Z} : f(x) = 0\}$.

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

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

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

[6] 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 $x_1^2 + \cdots + x_6^2$.

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 $X \to \infty$.[7]
3. For r_3, still have $\sum_{a \leq X^3} r_3(a) \sim C_3 X^3$ for first moment.[8]
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.[9]

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 $K \subseteq \mathbb{R}^6$.

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

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

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