Heuristics in Arithmetic—and randomness

Basic Notions Lectures: Dec 2, 9

Barry Mazur

What is a Basic Notion?

It's exciting to be giving a basic notions seminar—a seminar offering a type of reflection about mathematics that David Kazhdan introduced at Harvard many years ago.

What is a Basic Notion?

It's exciting to be giving a basic notions seminar—a seminar offering a type of reflection about mathematics that David Kazhdan introduced at Harvard many years ago.

The idea was not to offer the latest results, so much as to take *one single* notion or construction, or inspiring analogy, or heuristic, and show how it pervades different areas of mathematics.

What is a Basic Notion?

It's exciting to be giving a basic notions seminar—a seminar offering a type of reflection about mathematics that David Kazhdan introduced at Harvard many years ago.

The idea was not to offer the latest results, so much as to take *one single* notion or construction, or inspiring analogy, or heuristic, and show how it pervades different areas of mathematics.

I remember that Serre did that, giving one basic notions seminar, starting off with the word *homotopy*.

What is a Basic Notion?

It's exciting to be giving a basic notions seminar—a seminar offering a type of reflection about mathematics that David Kazhdan introduced at Harvard many years ago.

The idea was not to offer the latest results, so much as to take *one single* notion or construction, or inspiring analogy, or heuristic, and show how it pervades different areas of mathematics.

I remember that Serre did that, giving one basic notions seminar, starting off with the word *homotopy*.

I suppose Hermann Weyl could well have given a basic notions seminar in the spirit of his book *Symmetry*.

Basic Notions

Kazhdan's sense that basic notions are a crucial gateway to mathematical truth is coupled with his clear commitment to friendship as being essential for the best mathematical practice, so—in my lectures— I'm happy to touch on three projects with close mathematical friends—that connect to heuristics in arithmetic; first, commenting on work with:

- Lucia Caporaso and Joe Harris; *then with*
- Karl Rubin; *and the final part with*
- Karl Rubin and Sasha Shlapentokh.

Reasoning from Randomness

You ask yourself a question about some mathematical set-up and want to know how many instances of this set-up exist.

Reasoning from Randomness

You ask yourself a question about some mathematical set-up and want to know how many instances of this set-up exist.

You make a list of everything you know about the structure of it, and then...

Reasoning from Randomness

You ask yourself a question about some mathematical set-up and want to know how many instances of this set-up exist.

You make a list of everything you know about the structure of it, and then...

if everything else is random...

Reasoning from Randomness

You ask yourself a question about some mathematical set-up and want to know how many instances of this set-up exist.

You make a list of everything you know about the structure of it, and then...

if everything else is random...

you just compute—to get an estimate, which you then conjecture to be the actual estimate.

Reasoning from Randomness

You ask yourself a question about some mathematical set-up and want to know how many instances of this set-up exist.

You make a list of everything you know about the structure of it, and then...

if everything else is random...

you just compute—to get an estimate, which you then conjecture to be the actual estimate.

It's more hubristic than heuristic, since it seems to be making the assumption that your knowledge extends to all relevant structure (and everything else is random).

A Heuristic of Non-correlation and the *Self-Contradictory Heuristic*:

Are the operations of 'Addition' and 'Multiplication"

Correlated?

There's a natural (statistical) way of asking this question—leading to an empirical (and theoretical) project:

A Heuristic of Non-correlation and the *Self-Contradictory Heuristic*:

Are the operations of 'Addition' and 'Multiplication"

Correlated?

There's a natural (statistical) way of asking this question—leading to an empirical (and theoretical) project:

Is there any serious *correlational structure* regarding the multiplicative features (e.g., "roundness") of three whole numbers A, B, C if they are subject to the additive constraint:

$$\boxed{\text{A+B= C?}}$$

For example:

Let a, b, c be a triple of positive integers; these will play the role as *exponents.*

Consider the diophantine equation

$$A + B = C$$

where:

- A is allowed to be any positive integer that is a perfect a-th power,
- B a perfect b-th power and
- C a perfect c-th power.

So, for example, if

$$a = b = c = 2$$

then we're considering Pythagorean triples.

Counting these solutions:

Let X be a large positive integer, and $N(X)$ be the number of solutions of our diophantine equation

$$A + B = C$$

with $C \leq X$. What can we say about the behavior of $N(X)$ as a function of the bound X?

Counting these solutions:

Let X be a large positive integer, and $N(X)$ be the number of solutions of our diophantine equation

$$A + B = C$$

with $C \leq X$. What can we say about the behavior of $N(X)$ as a function of the bound X?

An optimistic heuristic—a sort of null hypothesis—is that the basic statistical behavior of $N(X)$ is dictated by the constraints on it that we *already know*.

The two sides, $A + B$ and C, of our diophantine problem:

$$A + B = C$$

are assumed "random," except, of course, for all our "prior" knowledge about them. So we must take an inventory of what we actually know:

- *Is there an systematic structure to the collection of solutions?*

The two sides, $A + B$ and C, of our diophantine problem:

$$A + B = C$$

are assumed "random," except, of course, for all our "prior" knowledge about them. So we must take an inventory of what we actually know:

- *Is there an systematic structure to the collection of solutions?*

  Well, if d is the least common multiple of the exponents a, b, c and (A, B, C) is a solution to our problem, i.e., a contributor to the number $N(X)$,

then for every integer

$$k = 1, 2, 3, \ldots \left(X/C\right)^{\frac{1}{d}}$$

we have that

- $$\left(k^d \cdot A,\ k^d \cdot B,\ k^d \cdot C\right)$$

  is also a solution.

Hypothesizing the systematic structure away:

Change our problem, and ask questions about the behavior of the function

$$N_o(X) := \text{the number of } \textit{relatively prime} \text{ triples } (A, B, C)$$

$$\text{that are solutions to our problem.}$$

Of course this will affect the collection of (A, B, C)'s that are in the game, but as we will see, not by much.

Formulating the probabilistic event:

We get a "hit," i.e., a solution to $A + B = C$ every time we get that the number $A + B - C$ is zero.

But—and this is the big assumption—

Viewing $A + B - C$ as randomly roaming through the allowable range which is roughly of size X as we run through our allowable triples (A, B, C),
the probability that any $A + B - C$ is zero is roughly X^{-1}.

So we do have (roughly)

$$X^{\frac{1}{a}} \cdot X^{\frac{1}{b}} \cdot X^{\frac{1}{c}} = X^{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}}$$

shots at this.

So the expected number of successes will be $\frac{1}{X}$ times $X^{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}}$,

Or:

$$X^{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}-1}.$$

To blur things a bit

given that we have been arguing quite naively, we might conjecture:

- When
$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}>1,$$
we should get:

Conjecture

$$X^{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}-1-\epsilon} < N_o(X) < X^{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}-1+\epsilon}$$

for any $\epsilon > 0$, and for $X >> 0$ (with the implied constant in "$>>$" depending on ϵ).

The Self-contradictory Heuristic

When

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1,$$

the above estimate would give us a *decreasing* number of hits as X tends to infinity; which doesn't make much sense at all. Call it:

The Self-contradictory Heuristic

and interpret it as:

The Self-contradictory Heuristic

When

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1,$$

the above estimate would give us a *decreasing* number of hits as X tends to infinity; which doesn't make much sense at all. Call it:

The Self-contradictory Heuristic

and interpret it as:

Conjecture

Fixing exponents a, b, c satisfying the inequality

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1,$$

there are only finitely many solutions to the diophantine problem

$$U^a + V^b = W^c$$

FLT, ABC

Of course, the classical *Last Theorem of Fermat* specifies a good deal more precise information than the above conjecture for the cases $a = b = c > 3$.

FLT, ABC

Of course, the classical *Last Theorem of Fermat* specifies a good deal more precise information than the above conjecture for the cases $a = b = c > 3$. This illustrates the structural shortcoming of this probabilistic heuristic: it is quintessentially probabilistic, and (it alone) could not get one to guess as *precise* a conjecture as Fermat's Last Theorem, even though it might offer, as plausible guess, some affirmation of the qualitative aspect of that Theorem.

The border line case: when $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1$

This involves just a handful of possibilities:
$(3, 3, 3), (2, 3, 6), (2, 4, 4)$ and their permutations; each of them have interesting stories.

All this motivates the work of Masser and Oesterlé with their wonderful, sweeping, ABC conjecture.

Non-Correlation

And all this above is motivated by the sentiment that relationships like

- $A + B = C$—or broadly put: *the operation of addition*—-and properties such as
- *powerfulness* or *roundness*—or broadly put: *multiplicative properties*

are statistically uncorrelated. . .

Non-Correlation

And all this above is motivated by the sentiment that relationships like

- $A + B = C$—or broadly put: *the operation of addition*—-and properties such as
- *powerfulness* or *roundness*—or broadly put: *multiplicative properties*

are statistically uncorrelated. . . at least once one takes into account certain elementary and evident correlations.

Hidden correlations: Artin's Conjecture about Primitive Root densities

The integer $a \neq 0, \pm 1$ is a primitive root for p (a prime not dividing a) if and only if for no prime q both:

1. $p \equiv 1 \mod q$, and
2. $a^{\frac{p-1}{q}} \equiv 1 \mod p$

are true. Artin first assumed that for different primes q conditions (1) and (2) are independent... making a density conjecture on the basis of this assumption. This was wrong (as illustrated by computations of Lehmer).

Hidden correlations: Artin's Conjecture about Primitive Root densities

The integer $a \neq 0, \pm 1$ is a primitive root for p (a prime not dividing a) if and only if for no prime q both:

1. $p \equiv 1 \mod q$, and
2. $a^{\frac{p-1}{q}} \equiv 1 \mod p$

are true. Artin first assumed that for different primes q conditions (1) and (2) are independent... making a density conjecture on the basis of this assumption. This was wrong (as illustrated by computations of Lehmer).
So... Artin took into account the dependence and revised his conjecture... and the revised conjecture remain unsolved.

Structural versus Statistical

Compare the conjectures we've just discussed with the statement of any structural theorem such as the *Pythagorean Theorem*, or *Unique Factorization for* $\mathbb{Z}$. Nothing could be more different! (*qualitative* versus structural)

Versions of the ABC conjecture with ABC-like non-correlations

guaranteeing multiplicative properties and additive properties are 'independent,' give evidence for, e.g.:

- The (generalized) Catalan problem where one looks for whole number solutions of

$$x^n - y^m = c \tag{1}$$

in the variables (x, y, n, m) with $x, y > 0$ and where $c \in \mathbb{Z}$ is a constant.

A simple application of the‘optimistic heuristic’

offers the guess that there should be on the order of

$$X^{\frac{1}{n}+\frac{1}{m}-1+o(1)}$$

solutions of Equation 2 for a fixed value of c.

Catalan

So when $n, m > 2$ we are facing the weird 'guess' that the expected number of solutions decreases as X increases: i.e., again the *self-contradictory heuristic* and again we interpret it as suggesting that we conjecture that:

Conjecture

(for such a choice of values of m and n) there are only finitely many solutions of

$$x^n - y^m = c \tag{2}$$

for any given c.

Classical Catalan

In particular, the classical Catalan Problem (1844) asks for pairs of consecutive perfect powers, and the answer (provided by Preda Mihâilescu in 2002) is that there is only one such pair, namely:

$$8 = 2^3 \quad \text{and} \quad 9 = 3^2.$$

'Reverse Engineering' the Conjecture of Mordell

The general effect of the 'optimistic conjecture' is to press the possibility that there are *relatively few solutions* of whatever problem is being considered. For example, let's try our rough calculus on the following problem:

> *For a polynomial* $g(x) \in \mathbb{Q}[x]$ *of degree* d *with rational coefficients and no multiple roots, how often is one of its values* $g(a)$ *for* $a \in \mathbb{Q}$ *a square in* $\mathbb{Q}$*?*

'Reverse Engineering' the Conjecture of Mordell

There are roughly X^2 rational numbers of height $\leq X$ and roughly X of them are squares. Roughly $X^{\frac{2}{d}}$ rational numbers of height $\leq X$ are in the image of $g(\mathbb{Q})$.

'Reverse Engineering' the Conjecture of Mordell

There are roughly X^2 rational numbers of height $\leq X$ and roughly X of them are squares. Roughly $X^{\frac{2}{d}}$ rational numbers of height $\leq X$ are in the image of $g(\mathbb{Q})$.

Our heuristic gets us to expect

$$X^{1+\frac{2}{d}-2}$$

'hits' of height $\leq X$. So, if $d \leq 2$, if there are no obvious other constraints, the heuristic tells us to expect infinitely many, while if $d >> 2$, finitely many.

The borderline cases $d = 3, 4$

are clearly problematic, for indeed there are elliptic curves with infinitely many rational points; but—of course— here there is a fundamental feature that has to be taken account of; namely, the group structure.

The borderline cases $d = 3, 4$

are clearly problematic, for indeed there are elliptic curves with infinitely many rational points; but—of course— here there is a fundamental feature that has to be taken account of; namely, the group structure.

The fact that the Mordell-Weil group is finitely generated seems to be the excuse for our rough calculus misbehaving for this case. More about this, in a moment.

When $d > 4$

there is no other corresponding structure that contributes to an infinity of rational points, and—indeed—our rough calculus is on target: if $d > 4$ this naive heuristic predicts that the (hyperelliptic) curve

$$y^2 = g(x)$$

has only finitely many rational points. In fact they do only have finitely many rational points—

—since these curves ($d > 4$) are of genus > 1, and all curves of genus > 1 were conjectured by Mordell (1922) to have only finitely many rational points, this being proved by Faltings (six decades later).

—since these curves ($d > 4$) are of genus > 1, and all curves of genus > 1 were conjectured by Mordell (1922) to have only finitely many rational points, this being proved by Faltings (six decades later).

Moreover, a theorem of Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang may be roughly interpreted as showing that most hyperelliptic curves of high genus have relatively few rational points.
(*Pencils of quadrics and the arithmetic of hyperelliptic curves*: http://arxiv.org/abs/1310.7692)

The Challenge:

Can one find a formulation of some 'non-correlation conjecture' that implies (all of) Mordell's Conjecture?

The Challenge:

Can one find a formulation of some 'non-correlation conjecture' that implies (all of) Mordell's Conjecture?

Noam Elkies' Response:

"Mordell's Conjecture is as easy as ABC"

N. Elkies, ABC $\Longrightarrow$ Mordell's Conjecture, International Mathematics Research Notices 1991, No. 7)

Random Matrix Heuristics

Every mathematician must have some favorite applications of reasoning from randomness. In number theory, my current favorite is the *Cohen-Lenstra heuristic* that began the great discussion about guesses for the average values of ideal class groups over various ranges of number fields.

Random Matrix Heuristics

Every mathematician must have some favorite applications of reasoning from randomness. In number theory, my current favorite is the *Cohen-Lenstra heuristic* that began the great discussion about guesses for the average values of ideal class groups over various ranges of number fields.

- Cohen-Lenstra: quadratic imaginary fields
- Cohen-Martinet-Malle and others:—a more general framework—where roots of unity are the sticking point(s).

Thought-Experiment

The *Cohen-Lenstra heuristic* arises by imagining the thought-experiment of fabricating an ideal class group by a *random process* in terms of its generators and relations, subject to the prior constraints that reflect everything we know about the way in which the ideal class group appears—

Thought-Experiment

The *Cohen-Lenstra heuristic* arises by imagining the thought-experiment of fabricating an ideal class group by a *random process* in terms of its generators and relations, subject to the prior constraints that reflect everything we know about the way in which the ideal class group appears—

e.g., as if some random spirit entertained him-or-her self by building these ideal class groups, randomly in a devil-may-care manner dreaming them up as quotients of *an abstract model of* "an" idele class group.

Any Random matrix heuristic

applied to finding statistics for the structure of some general group invariant A (attached to a category of 'things,') will always start with a thought-experiment that imagines how that group invariant is constructed. E.g., is it a quotient

$$\mathbb{Z}^m \xrightarrow{M} \mathbb{Z}^n \to A \to 0?$$

where M is some matrix—constrained to have particular features to make the cokernels look like such A's?

Any Random matrix heuristic

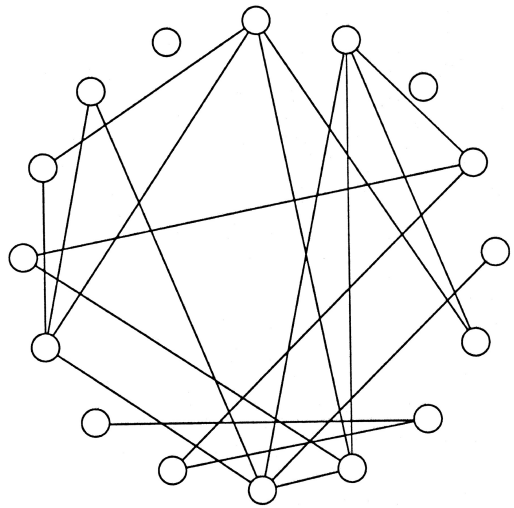
applied to finding statistics for the structure of some general group invariant A (attached to a category of 'things,') will always start with a thought-experiment that imagines how that group invariant is constructed. E.g., is it a quotient

$$\mathbb{Z}^m \xrightarrow{M} \mathbb{Z}^n \to A \to 0?$$

where M is some matrix—constrained to have particular features to make the cokernels look like such A's?

If so, assume that such M's are random but constrained to have those properties and then... compute.

Random graphs and "sandpile groups"



$$\mathsf{Z}[\text{Vertices}] \xrightarrow{\text{Laplacian}} \mathsf{Z}[\text{Vertices}] \longrightarrow \boxed{\text{Cokernel}} \to 0$$

That cokernel has many names:

$$\boxed{\text{Cokernel}} = \text{“Sandpile group”} = \text{“Jacobian”} = \text{“Picard group”}$$

of the graph

What is the probability that an "Erdos-Rényi" graph on n vertices with independent edge-probabilities q has its sandpile group isomorphic to a group group G?

—Cohen-Lenstra-type heuristics, again—

Melanie Wood: gives precise answer (for p-Sylow subgroups)

Graphs with nodes= elliptic curves; and edges= isogenies

I'm thankful to Ari Shnidman for emailing me yesterday about a result of Nathaniël Munier and his, where for p and q distinct primes, they consider $X_{p,q}$, the $(q+1)$-regular graph whose nodes are supersingular elliptic curves over the prime field F_p and whose edges are q-isogenies.

Graphs with nodes= elliptic curves; and edges= isogenies

I'm thankful to Ari Shnidman for emailing me yesterday about a result of Nathaniël Munier and his, where for p and q distinct primes, they consider $X_{p,q}$, the $(q+1)$-regular graph whose nodes are supersingular elliptic curves over the prime field F_p and whose edges are q-isogenies.

For fixed p, they show that the ℓ-Sylow subgroup of the sandpile group (of $X_{p,q}$ (as q tends to infinity) disagrees with the Cohen-Lenstra heuristic in this context. This is neat, and I hope Ari can say more about this!

Empirical Number Theory

Whether the Cohen-Lenstra heuristics work or not, they do have a firm place in the toolkit of conjectures that might be informative (one way or other) as guides for reflections and experiments in that empirical branch of number theory.

Some words about elliptic curves, abelian varieties

Abelian varieties are projective algebraic varieties that have an algebraically defined group structure—(surprisingly) these are all commutative.

Some words about elliptic curves, abelian varieties

Abelian varieties are projective algebraic varieties that have an algebraically defined group structure—(surprisingly) these are all commutative.

In dimension one, they're called **elliptic curves** and any of these can be represented as plane cubics, with a unique point at infinity (taken to be the origin of their group structure). An old-fashioned phrase alluding to, and explaining, their group structure is the chord-and-tangent-process.

Mordell-Weil groups

If an abelian variety A is defined over a field K its *set* of K-rational points $A(K)$ is a (naturally) a commutative group—called it's **Mordell-Weil group**.

Mordell-Weil groups

If an abelian variety A is defined over a field K its *set* of K-rational points $A(K)$ is a (naturally) a commutative group—called it's **Mordell-Weil group**.

If K is a number field, then $A(K)$ is a finitely generated abelian group—

thanks to *Mordell* (who proved this for elliptic curves over Q)—

and to *Weil* (who proved the general statement)—

Mordell-Weil groups

If an abelian variety A is defined over a field K its *set* of K-rational points $A(K)$ is a (naturally) a commutative group—called it's **Mordell-Weil group**.

If K is a number field, then $A(K)$ is a finitely generated abelian group—

thanks to *Mordell* (who proved this for elliptic curves over Q)—

and to *Weil* (who proved the general statement)—

The rank of $A(K)$ rank is called the **MW-rank of A over K**.

A heuristic for boundedness of ranks of elliptic curves

This is the title of an article by *Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood* which contains a random matrix heuristic argument leading to the remarkable guess that:
there is a finite upper bound to the Mordell-Weil ranks of all elliptic curves over $\mathbb{Q}$.

A heuristic for boundedness of ranks of elliptic curves

This is the title of an article by *Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood* which contains a random matrix heuristic argument leading to the remarkable guess that:
there is a finite upper bound to the Mordell-Weil ranks of all elliptic curves over $\mathbb{Q}$.

This guess was originally made by Honda only for families of quadratic twists of a single elliptic curve—and that was not even believed at the time by all number theorists for that special case!

The heuristic offers a guess for an explicit bound

Park, Poonen, Voight and Wood conjecture that: The number of elliptic curves with 'naive' height H and Mordell-Weil-rank $\geq r$ is no greater than

$$H^{\frac{21-r}{24}+o(1)}$$

save for possibly finitely many elliptic curves.

The self-contradictory heuristic, again

The conjecture of *Park, Poonen, Voight and Wood* reads, when $r > 21$, as the weird statement that:

the number of elliptic curves with 'naive' height H and Mordell-Weil-rank $\geq r$ is **declining** as H is growing.

This is quite naturally interpreted as offering courage to:

Conjecture

There are only finitely many elliptic curves defined over $\mathbb{Q}$ *with Mordell-Weil rank* > 21.

Record MW-ranks under the above estimate:

rank $\geq$	year	Author(s)
3	1938	*Billing*
4	1945	*Wiman*
6	1974	*Penney – Pomerance*
7	1975	*Penney – Pomerance*
8	1977	*Grunewald – Zimmert*
9	1977	*Brumer – Kramer*
12	1982	*Mestre*
14	1986	*Mestre*
15	1992	*Mestre*
17	1992	*Nagao*
19	1992	*Fermigier*
20	1993	*Nagao*
21	1994	*Nagao – Kouya*

Record MW-ranks above the above estimate:

rank $\geq$	year	Author(s)
22	1997	*Fermigier*
23	1998	*Martin – McMillen*
24	2000	*Martin – McMillen*
28	2006	*Elkies*

Noam Elkies' elliptic curve with MW-rank ≥ 28:

Elkies (2006)

$$y^2 + xy + y =$$

$$x^3 - x^2 -$$

$$2006776241557552658503320820933854275093023031217895650 2x +$$

$$+ 3448161179503055646703298569039072037485594435 9$$

$$3191803612660082962919394487322434 29$$

Serge Lang's *minimalist* View: Rational Points are Rare!

Conjectures (and some results) suggest that, on the whole, algebraic varieties over a number field K tend not to have all that many K-rational points unless either

- there is some specific algebraic geometric structure generating them, e.g., a group structure could 'produce' loads of rational points from a few of them.
- For example, (nontrivial) Algebraic groups over a number field have *Zariski-dense* K-rational points for some number field K containing the field over which they are defined.

Hence: infinitely many of them.

Or possibly, and this is a bit more mysterious:

- a functional equation (proved, or conjectured) and a corresponding root number computation predicts the parity of the rank of a Mordell-Weil group (which in many cases allows one to expect the existence of more rational points than is in evidence without this prediction).

But lacking either reason for rational points to be abundant, the sense is that they are scarce.

For example, if V is an algebraic variety defined over $\bar{Q}$, that admits a non-constant mapping $G \to V$ of where G is a connected positive dimensional algebraic group, then there is a number field K over which V is defined and possesses infinitely many K-rational points.

Conjecture

(Serge Lang) Otherwise not!

The "Strong Lang Conjecture"

There are variants of such conjectures, one of them known as SLC: the "Strong Lang Conjecture".

An implication of the Strong Lang Conjecture (SLC) is

Conjecture

Any algebraic variety V over $\bar{\mathbb{Q}}$ that does not contain a positive-dimensional image of an algebraic group (over $\bar{\mathbb{Q}}$) possesses only finitely many K-rational points over any number field K (over which it is defined).

Strong uniformity

Assuming the Strong Lang Conjecture, Lucia Caporaso, Joe Harris and I proved the following consequence:

Theorem

Let $g > 1$. The Strong Lang Conjecture implies that there is a (finite) bound $N(g)$ with the property that for every number field K only finitely many curves of genus g defined over K have more than $N(g)$ K-rational points.

The curious point here is that $N(g)$ doesn't even depend on the field K.

Of course, such a consequence of SLC might force one to have second thoughts about the likelihood of SLC being true. But let us continue this discussion supposing that SLC does hold, and so the following limit is finite:

$$N(g) := \max_{K \subset \bar{\mathbb{Q}}} \limsup_{C:\ \text{curves}/K\ \text{of genus}\ g} |C(K)|.$$

Lower bounds for $N(g)$

It is easy to see that

$$N(g) \geq 2g + 2 \text{ if } g > 1,$$

but not much more is known in the way of lower bounds. Less, of course, is known in the way of upper bounds.

The record lower bounds for genus 2 and 3, so far are:

- $N(2) \geq 226$ (Genya Zaytman) and
- $N(3) \geq 100$ (Noam Elkies).

Even stronger uniformity?

My co-authors (Lucia Caporaso, and Joe Harris) and I wonder whether even more uniformity might not be the case: we feel that the right 'parameter' to consider is:

Definition

$\mathcal{N}_* := \liminf_{g\to\infty} N(g)/g.$

Definition

$\mathcal{N}^* := \limsup_{g\to\infty} N(g)/g.$

Higher lower bounds

Curves in $\mathrm{P}^1 \times \mathrm{P}^1$ of bidegree $(2, g+1)$ are of arithmetic genus g. They form a linear system of dimension $3(g+2)-1$.

Given $3(g+2)-1$ general points

$$p_1, \ldots, p_{3g+5} \in \mathrm{P}^1 \times \mathrm{P}^1(\mathrm{Q}),$$

accordingly, there will be a smooth curve C defined over Q and passing through them.

And since C is a general hyperelliptic curve, its automorphism group is equal to $\mathrm{Z}/2$, consisting of the identity and the hyperelliptic involution; and since no two of the points p_i lie in the same fiber of $\mathrm{P}^1 \times \mathrm{P}^1$ over P^1, no two are conjugate under the automorphism group of C.

We have accordingly:

$$3 \leq \mathcal{N}_* \leq \mathcal{N}^*. \tag{3}$$

Some natural questions:

- Is $\mathcal{N}^*$, or perhaps only $\mathcal{N}_*$, or neither of them, finite?
- Are both inequalities in

$$3 \leq \mathcal{N}_* \leq \mathcal{N}^*$$

equalities? (or is one of them, or neither)?

Uniformity in moduli parameters?

- Let $M^*_{g,n}$ denote the moduli space of projective smooth curves of genus g with n *distinct* marked rigid points.

  For K a number field let $d_{g,n}(K)$ denote the dimension of the Zariski-closure in $M^*_{g,n}$ of the set of K-rational points $M^*_{g,n}(K)$.

  Now define

$$d_{g,n} := \max_K d_{g,n}(K)$$

  where the maximum is taken over all number fields K.

Uniformity in moduli parameters?

Conjecture SLC implies that:

For fixed $g \geq 2$—if $n \gg_g 0$, then

$$d_{g,n} = 0.$$

Might $d_{g,n}$ be decreasing (albeit not necessarily strictly) for fixed g and increasing n?

Here is a far-out question:

Question

*Call a curve of genus g defined over K a K-***outlier** *if it has more than $N(g)$ K-rational points. Is there anything waiting to be said about the number of K-outliers as a function of K?*

What about quadratic uniformity?

Quadratic Points

A K-**quadratic point** of a curve C over a field K is a *rational point* of C over a quadratic field extension L/K.

There are two ways for a curve C of genus > 1 defined over a number field K to have loads (i.e., infinitely many) of quadratic points (over K):

- C could be *hyperelliptic* meaning that it is a degree two cover of the projective line.
- C could be *bielliptic* meaning that it is a degree two cover of an elliptic curve that happens to have infinitely many K-rational points.

Faltings' Theorem

If it is neither hyperelliptic nor bielliptic (and of genus > 1)—then Faltings has proved that C has only finitely many K-quadratic points.

So... how many?

Is there 'quadratic uniformity" independent of the base number field?

Conjecture: There's a finite upper bound $N_2(g)$ such that for *any* number field K there are only finite many curves defined over K that are of genus $g > 1$ and neither hyperelliptic nor bielliptic and have more than $N_2(g)$ K-quadratic points.

Quadratic advances. . .

Dan Abramovich tells me that the argument of Caporaso, Harris and myself, coupled with his paper with José Voloch

Lang's conjectures, fibered powers, and uniformity. New York J. Math. 2 (1996), 20-34

should prove:

Theorem

SLC also implies the above Conjecture.

1. This theorem isn't explicitly written down; so a neat project to be done.

2. Thinking about possible projects: More generally, say that a curve has **bi-gonality** d if every mapping to P^1 (alias: rational function) or to an elliptic curve has degree $\geq d$. (This is a *neologism*.)

Degree d rational points

Conjecture: There's a finite upper bound $N_d(g)$ such that for *any* number field K there are only finite many curves defined over K that are of genus $g > 1$ and are of bi-gonality $> d$ have more than $N_d(g)$ points rational in field extensions of degree $\leq d$ over K.

Degree d rational points

Conjecture: There's a finite upper bound $N_d(g)$ such that for *any* number field K there are only finite many curves defined over K that are of genus $g > 1$ and are of bi-gonality $> d$ have more than $N_d(g)$ points rational in field extensions of degree $\leq d$ over K.

1. Another neat project: to show that SLC implies this conjecture. (?)
2. Comment on the very recent determination of all Q-quadratic isogenies of elliptic curves (defined over Q).

Heuristics in Arithmetic—and randomness

Basic Notions Lecture: Dec 9

Barry Mazur

What is a ‘heuristic’ in Mathematics?

I’m thankful to Yuval Flicker for asking that question in our chat after my lecture last Thursday. I said that I’d take this as homework and would bring it to my lecture today. It—or least a start to it— is attached in the chat.

No *new* Rational Points

With Karl Rubin, I've been considering a 'relative question' that has a field extension in the game:

Definition

Let V be a variety defined over K.

1. V is **diophantine stable** for the field extension L/K if $V(L) = V(K)$; that is, if V acquires no *new* rational points when one extends the base field from K to L.

2. A field extension L/K **belongs to** V if there is an L-rational point of V that is not defined over any properly smaller field containing K.

Fixing the field extension L/K

Proposition

(Suppose SLC.) Fix $g > 1$ and let L/K be any number field extension of degree larger than $N(g)$.

Then L/K belongs to only finitely many (isomorphism classes of) curves C over K of genus g.

Question

Let X and Y be two absolutely irreducible curves defined over K that have the same set of field extensions L/K belonging to them.

Is it true that X is birationally equivalent to Y over the algebraic closure $\bar{K}$?

Fixing the curve—or fixing an abelian variety

The "minimalist philosophy" leads us to the following question.

Question

If C is a curve of genus > 0 (resp: if A is an abelian variety) over K, ℓ is an odd prime number, and m is a positive integer, is it the case that

(among all cyclic Galois extensions of K of degree ℓ^m, ordered by conductor)

the cyclic Galois extensions of K of degree ℓ^m that are diophantine stable for C (resp. A) are of density 1 ?

Focusing on abelian varieties

Karl Rubin and I proved the following embarrassingly weak theorem in the direction of answering this question

Theorem

If A/K is a simple abelian variety such that $\mathrm{End}_{\bar{K}}(A) = \mathrm{End}_K(A)$, then:

there is a set S of prime numbers of positive density such that for all $\ell \in S$ and for all positive integers m there are infinitely many cyclic Galois extensions of K of degree ℓ^m that are diophantine stable for A.

The weakness of the theorem

Unfortunately we cannot replace the phrase "infinitely many" in the statement of our theorem by "a positive proportion" (where 'proportion' is defined by organizing these cyclic extensions by size of conductor).

The weakness of the theorem

Unfortunately we cannot replace the phrase "infinitely many" in the statement of our theorem by "a positive proportion" (where 'proportion' is defined by organizing these cyclic extensions by size of conductor).

If we order the extensions by size of conductor and consider what we have proved for a given ℓ^m, among the first X of these we get at least—

$$X/\log^{\alpha} X$$

of them as $X \to \infty$ (for a small, but positive, α).

A comment:

When $K/\mathbb{Q}$ is quadratic, the cyclic ℓ^m extensions of K that are Galois dihedral extensions of $\mathbb{Q}$ are potentially a source of systematic diophantine instability but they are of density 0 in all cyclic ℓ^m extensions of K.

Random Matrix Heuristics again

The following conjectures and predictions about elliptic curves E over $\mathbb{Q}$ are suggested by the random matrix heuristic.

Random Matrix Heuristics again

The following conjectures and predictions about elliptic curves E over Q are suggested by the random matrix heuristic. This involves work of

- Conrey, Keating, Rubinstein, and Snaith for $p = 2$, and
- David, Fearnley, and Kisilevsky and also Fearnley, Kisilevsky, and Kuwata for p odd.

For $f(X), g(X)$ functions of a real variable X, we write $f(X) \sim g(X)$ if

$$\lim_{X \to \infty} \frac{f(X)}{g(X)} = 1.$$

Conjecture (DFKK)

Fix E an elliptic curve over $\mathbb{Q}$.

For a prime $p > 2$, and X a positive number, define:

$N_{E,p}(X) = N_p(X) :=$ *the number of cyclic degree p extensions $L/\mathbb{Q}$ of conductor $\leq X$ that are diophantine un-stable for E.*

Then there are nonzero constants $b_{E,p}, c_{E,p}$ for which

- $N_{E,3}(X) \sim b_{E,3}\sqrt{X}\log(X)^{c_{E,3}}$,
- $N_{E,5}(X) \sim b_{E,5}\log(X)^{c_{E,5}}$,

and ...

For $p \geq 7$

- $N_{E,p}(X)$ is bounded independently of X if $p \geq 7$.

  (I.e., there are only finitely many diophantine unstable cyclic p-extensions $L/\mathbb{Q}$ (for E) if $p \geq 7$.)

Towards a "modular symbol" heuristic

In contemplating (in effect) how weak our diophantine stability theorem was—and inspired by the random matrix prediction of David, Fearnley and Kisilevsky—Karl Rubin and I turned to the structure of modular symbols as determining special values of L-functions relevant—conditional on standard conjectures—to diophantine stability.

We have lectured about this before so here I will jump to the essential part of our heuristic, which:

We have lectured about this before so here I will jump to the essential part of our heuristic, which:

- is a strikingly weak statistical hypothesis supported by the substantial relevant data already available, and

We have lectured about this before so here I will jump to the essential part of our heuristic, which:

- is a strikingly weak statistical hypothesis supported by the substantial relevant data already available, and
- makes predictions that are of significantly broader generality than the random matrix heuristics stated above, but that are in agreement with them, in the cases where they overlap.

The essential part of our heuristic

Fix a 'pair' (E, d) where E is an elliptic curve over $\mathbb{Q}$ and d is a positive integer (> 1).

For a real number X we want to consider the set

$$\mathcal{L}(X)$$

of all cyclic extensions $L/\mathbb{Q}$ of order d of conductor $m_L < X$.

Put

$$\mathcal{L} = \cup_{X<\infty}\mathcal{L}(X),$$

i.e., the set of all cyclic extensions $L/\mathbb{Q}$ of order d.

Rational integer "Theta-values" coming from the "analytic number theory of elliptic curves"

(That is, coming from special values of L-functions attached to elliptic curves)

For any elliptic curve E over $\mathbb{Q}$ and cyclic Galois extension $L/\mathbb{Q}$ in $\mathcal{L}$ there is an integral valued function

$$\theta_{E,d;L/\mathbb{Q}} = \theta : \mathrm{Gal}(L/\mathbb{Q}) \rightarrow \mathbb{Z}$$

with the following property:

For any injective homomorphism

$$\chi : \mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \mathbb{C}^*$$

(viewed as primitive Dirichlet character of conductor m)
we have that:
the special value of the L-function of E, twisted by χ at $s = 1$:

$$L(E, \chi, 1)$$

is (up to a nonvanishing, and elementary, factor) equal to

$$\sum_{\gamma \in \mathrm{Gal}(L/\mathbb{Q})} \chi(\gamma)\theta(\gamma).$$

A Consequence, conditional on a standard conjecture (BSD):

Let $L/\mathbb{Q}$ be the cyclic extension of degree d and conductor m 'cut out by the Dirichlet character χ, then:

$$\boxed{L/\mathbb{Q} \text{ is diophantine unstable for } E}$$

$$\overset{BSD}{\leftrightarrow}$$

$$\boxed{\sum_{\gamma \in \mathrm{Gal}(L/\mathbb{Q})} \chi(\gamma) \cdot \theta_E(\gamma) \;=\; 0.}$$

Hence, for example, if $d = p$, a prime:

$L/\mathbb{Q}$ is diophantine unstable for E

$\overset{BSD}{\Leftrightarrow}$

The values $\Theta_{E;L/Q}(\gamma)$ are the same for *all* $\gamma \in \mathrm{Gal}(L/\mathbb{Q})$

Because. . .

Lemma

We have

$$\sum_{\gamma \in G} \chi(\gamma)\theta(\gamma) = 0 \iff \theta(\gamma) = \theta(\sigma)$$

for all $\gamma, \sigma \in \mathrm{Gal}(L/\mathbb{Q})$.

Proof.

The only Q-linear relation among the values of χ (i.e., the p-th roots of unity) is that their sum is zero. It follows that the sum over γ is zero if and only if all the 'theta-values' $\theta(\gamma)$ are equal. $\square$

Distributions of θ-values

Consider real cyclic extensions $L/\mathbb{Q}$ of fixed degree $d \geq 3$ and varying conductor m.

Distributions of θ-values

Consider real cyclic extensions $L/\mathbb{Q}$ of fixed degree $d \geq 3$ and varying conductor m.

The Theta-values $\theta(\gamma)$ for (say, odd) degree d and conductor m are a sum of $O(\varphi(m))$ modular symbols

$$\boxed{[a/m]_E \quad \in \quad \mathbb{Z}}$$

which (in average; taken over all m and d) have a Gaussian distribution.

SO: if these "Theta-values" $\theta(\gamma)$ were the sums of $O(\varphi(m))$ *randomly chosen* modular symbols one would expect that:

(?) The distribution of (elementarily normalized) theta-values ranging over all cyclic Galois extensions of Q of degree d should also be Gaussian... at least for large d. **(?)**

SO: if these "Theta-values" $\theta(\gamma)$ were the sums of $O(\varphi(m))$ *randomly chosen* modular symbols one would expect that:

(?) The distribution of (elementarily normalized) theta-values ranging over all cyclic Galois extensions of Q of degree d should also be Gaussian... at least for large d. **(?)**

But...

Calculations do not support this expectation, at least not for small values of d.

However, calculations do support (thankfully) our weaker conjecture that I will describe later this lecture (after I show some of our data) and which:

Calculations do not support this expectation, at least not for small values of d.

However, calculations do support (thankfully) our weaker conjecture that I will describe later this lecture (after I show some of our data) and which:
is *more than strong enough for our purposes*.

Calculations do not support this expectation, at least not for small values of d.

However, calculations do support (thankfully) our weaker conjecture that I will describe later this lecture (after I show some of our data) and which:
is *more than strong enough for our purposes*.

Define the *normalized θ-coefficient*

$$\tilde{\theta}_{E;L/\mathbb{Q}}(\gamma) = \tilde{\theta}(\gamma) := \frac{\theta(\gamma)\sqrt{d}}{\sqrt{\varphi(m)\log(m)}}.$$

Some Data

For each of the three elliptic curves 11A1, 37A1, and 32A1 (in the notation of Cremona's tables) and for five (prime) values of d, we computed the first (approximately) 50,000 normalized θ-coefficients $\tilde{\theta}(\gamma)$, with $L/\mathbb{Q}$ ordered by conductor and γ generic [this involves a detail which we can discuss].

Some Data

For each of the three elliptic curves 11A1, 37A1, and 32A1 (in the notation of Cremona's tables) and for five (prime) values of d, we computed the first (approximately) 50,000 normalized θ-coefficients $\tilde{\theta}(\gamma)$, with L/Q ordered by conductor and γ generic [this involves a detail which we can discuss].

The resulting maybe-distributions are shown in Figures 1 through 3 below.

Some Data

For each of the three elliptic curves 11A1, 37A1, and 32A1 (in the notation of Cremona's tables) and for five (prime) values of d, we computed the first (approximately) 50,000 normalized θ-coefficients $\tilde{\theta}(\gamma)$, with $L/\mathbb{Q}$ ordered by conductor and γ generic [this involves a detail which we can discuss].

The resulting maybe-distributions are shown in Figures 1 through 3 below.

As d grows these maybe-distributions

$$\Lambda_{E,d}$$

approach the "expected" normal distribution, shown as the dashed line in each figure.

$\Lambda_{E_{11A1},d}$

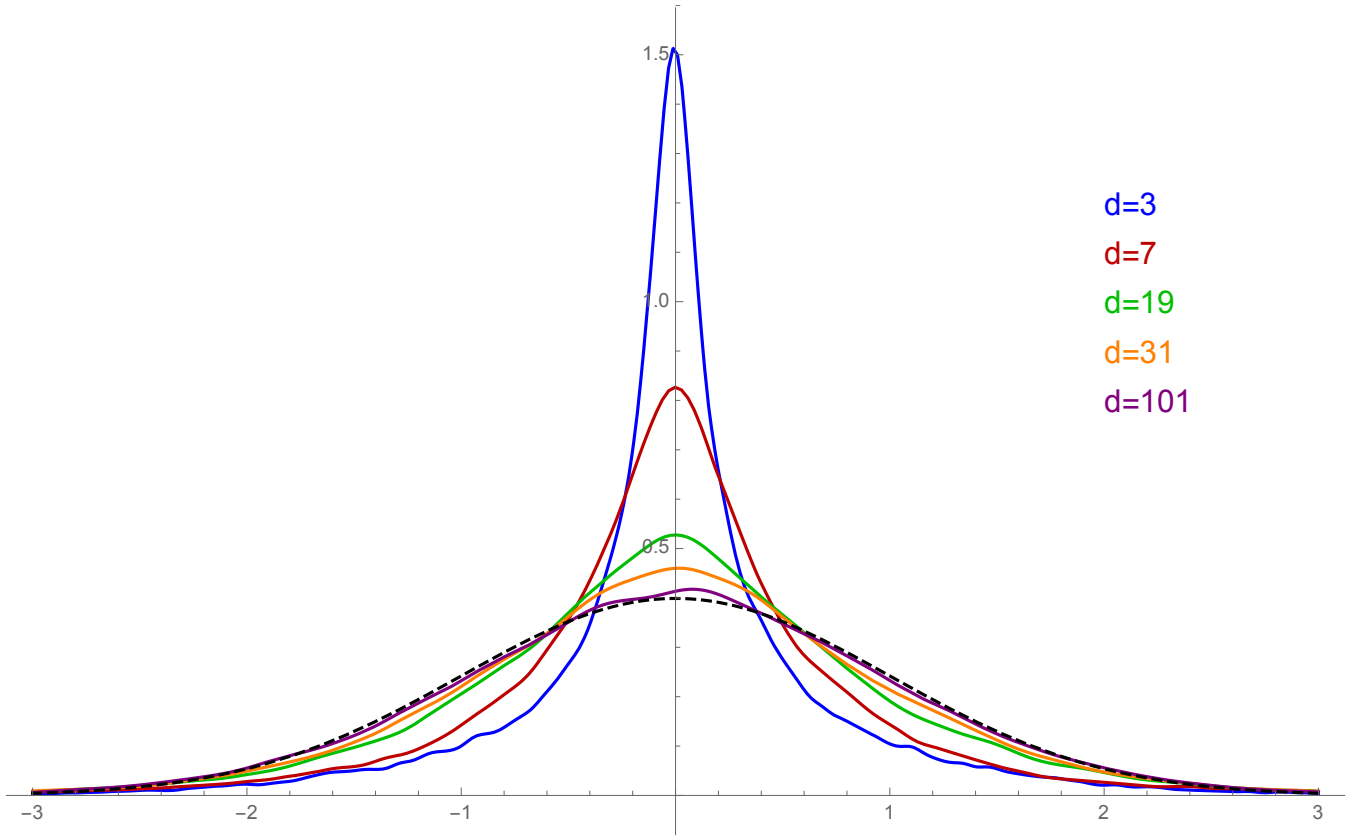


Figure: Distribution of normalized θ-coefficients for $E = 11A1$ and varying d.

$\Lambda_{E_{37A1},d}$

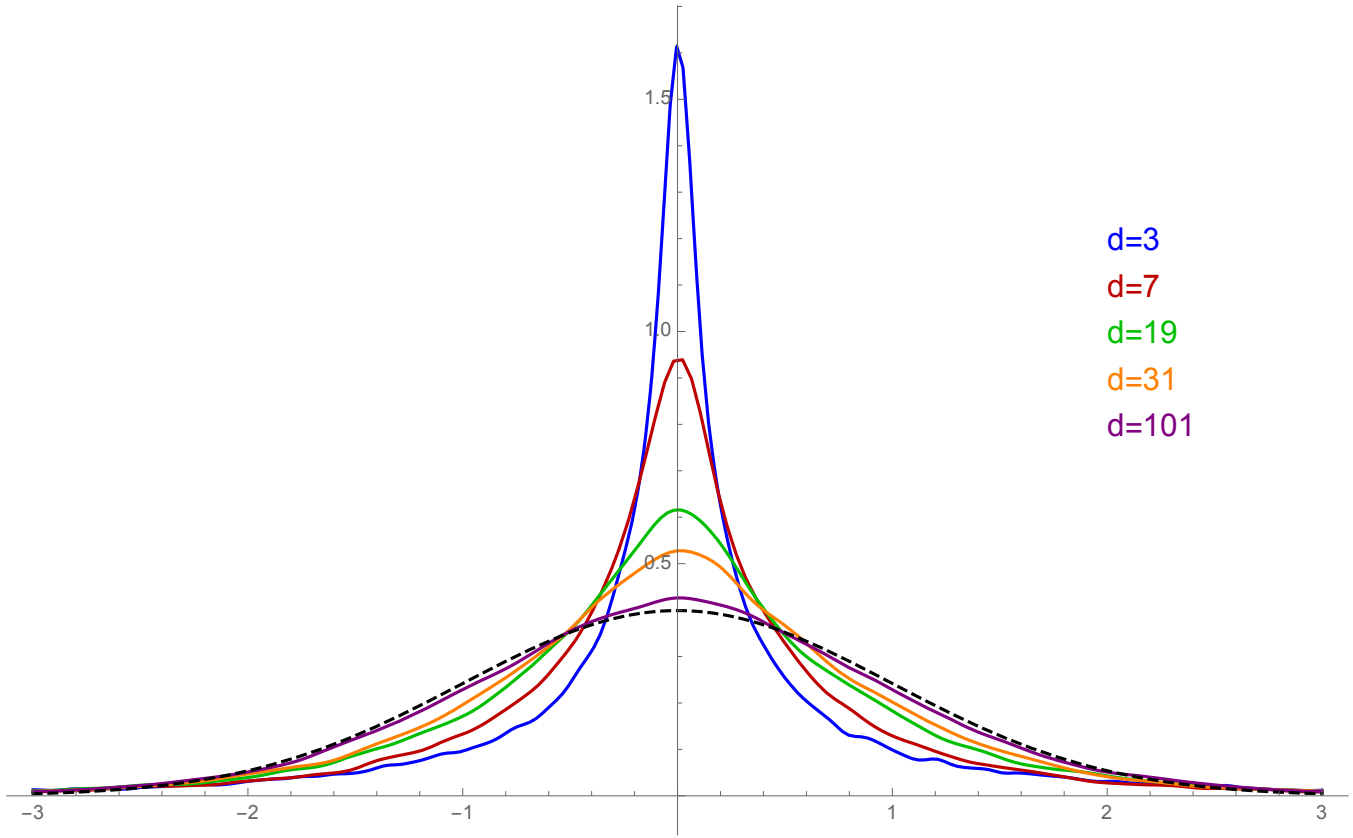


Figure: Distribution of normalized θ-coefficients for $E = 37A1$ and varying d.

$\Lambda_{E_{32A1},d}$

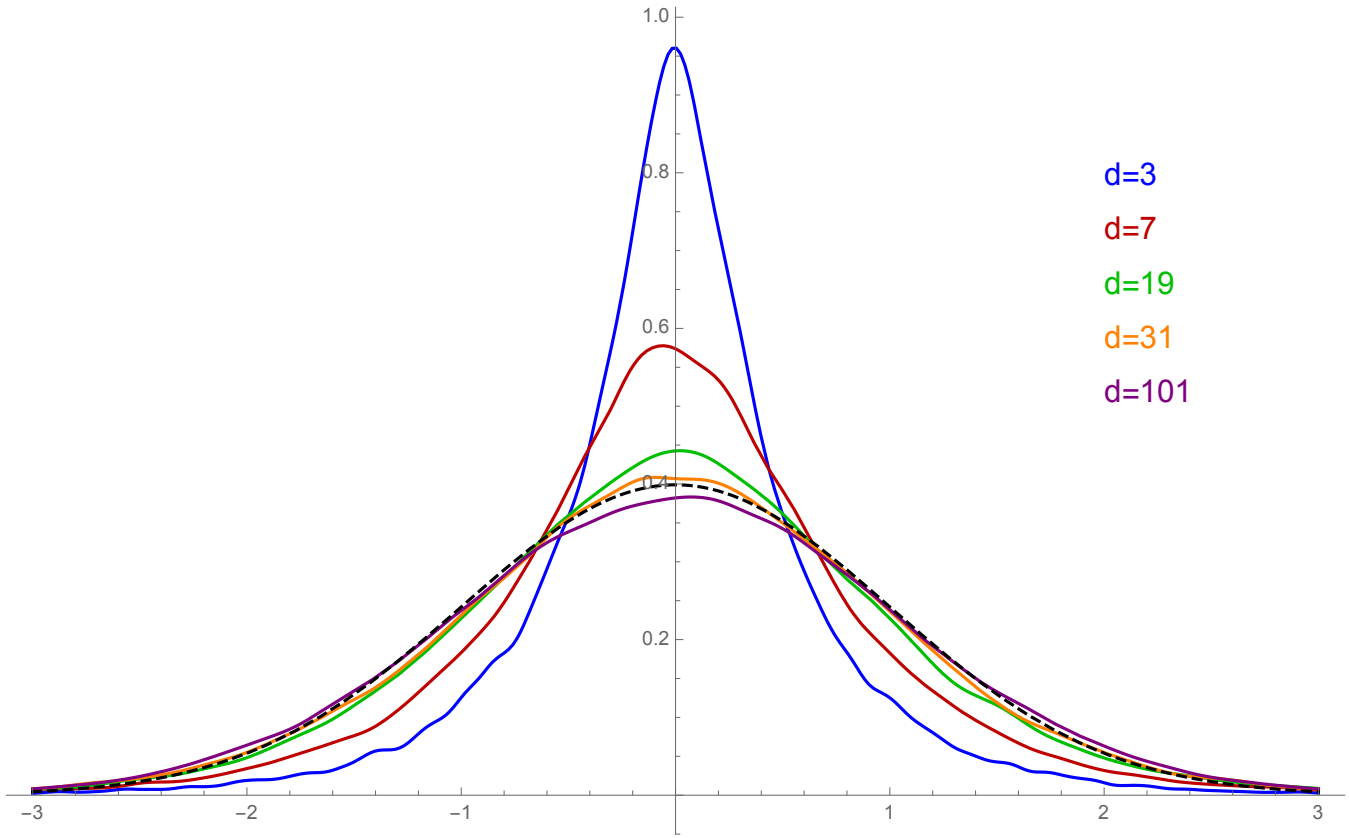


Figure: Distribution of normalized θ-coefficients for $E = 32A1$ and varying d.

What are these 'maybe–distributions' $\Lambda_{E,d}$?

We need *not* (and do not) conjecture that the distributions

$$\boxed{\Lambda_{E;d,m} \text{ for fixed } d \text{ and increasing } m}$$

even converge as m tends to infinity!

BUT: for large enough d do they, in fact, converge? If so what are these distributions? As d, and m tend to infinity do these values converge to a Gaussian distribution?

A weak conjecture suffices

All we conjecture, and all we need to conjecture—for the consequences we draw—is that

- there is a mild upper bound for these data sets, and
- the most minimal type of non-correlation between theta coefficients attached to a given L/Q.

Data sets

For

$$d \geq 3,$$
$$\alpha, \beta \in \mathrm{R}, \text{ and}$$
$$X \in \mathrm{R}_{>0},$$

let $\Sigma_{d,\alpha,\beta}(X)$ be the collection of data (counted with multiplicity) defined as follows:

$$\boxed{\Sigma_{d,\alpha,\beta}(X) :=}$$

the set of values

$$\{\tilde{\theta}(\gamma) m_L^{\alpha} \log(m_L)^{\beta}\}$$

where $\gamma \in \mathrm{Gal}(F/\mathbb{Q})$ and $L/\mathbb{Q}$ runs through real, cyclic extensions of degree d and conductor $< X$.

Uniform boundedness

Conjecture

There is a (uniform!) upper bound $B_E > 0$ *and for every* $d \geq 3$ *there are) 'exponents'* $\alpha_d, \beta_d \in \mathrm{R}$ *such that*

1. *for every real open interval* (a, b),

$$\limsup_{X \to \infty} \frac{\#\{\Sigma_{d,\alpha_d,\beta_d}(X) \cap (a,b)\}}{\#\Sigma_{d,\alpha_d,\beta_d}(X)} < B_E(b-a),$$

2. $\{\alpha_d \varphi(d) : d \geq 3\}$ *is bounded, and* $\lim_{d\to\infty} \beta_d = 0$.

Random matrix theory heuristics

(alluded to) suggest that $\boxed{\text{for } d = 3}$ and every real open interval (a, b),

$$\limsup_{X \to \infty} \frac{\#\{\Sigma_{d,\alpha_d,\beta_d}(X) \cap (a, b)\}}{\#\Sigma_{d,\alpha_d,\beta_d}(X)} < B_d(b - a), \qquad (4)$$

with $\alpha_3 = 0$, $\beta_3 = 3/4$ and a sufficiently large B_3.

Empirical data suggest (4) holds for **all** d

with

- $\alpha_d = 0$,
- β_d converging to zero for large d and
- B_d bounded for large d.

Taking B_E to be the maximum of the B_d leads to the statement of our conjecture.

Here is a heuristic shorthand description of the above Conjecture

There is an upper bound $B_E > 0$ such that for

- every cyclic extension F/Q of degree $d \geq 3$,
- but we exclude the (few) elements $\gamma \in \mathrm{Gal}(F/\mathrm{Q})$ that we call **special**$^-$ in our paper; and
- every real interval $(a, b) \ldots$

we conjecture an upper measures for 'likelihood'

We define the "**upper measure for the likelihood that the Theta values $\tilde{\theta}(\gamma)$ associated to some extension $L/\mathbb{Q}$ lies in the interval (a, b),**" to be

we conjecture an upper measures for 'likelihood'

We define the "**upper measure for the likelihood that the Theta values $\tilde{\theta}(\gamma)$ associated to some extension $L/\mathbb{Q}$ lies in the interval (a, b),**" to be

$$B_E(b-a)m_L^{\alpha_d}\log(m_L)^{\beta_d},$$

where B_E, α_d, β_d are as in our Conjecture.

Explain how this is used.

"Log-noncorrelation"

Recall: If $d = p$, a prime:

$$\boxed{L/\mathbb{Q} \text{ is diophantine unstable for } E}$$

$$\overset{BSD}{\Longleftrightarrow}$$

$$\boxed{\text{the Theta-values } \Theta_{E;L/Q}(\gamma) \text{ are } \textit{the same} \text{ for all } \gamma \in \mathrm{Gal}(L/\mathbb{Q})}$$

SO: if $p >> 0$ there must be a *lot* of correlation to get diophantine un-stability!

"Log-noncorrelation"

That is, if the probability that two Theta-values are equal is $\frac{1}{10}$ and if there is *complete non-correlation* the probability that *all* $p-1$ *Theta-values are equal* would be $\frac{1}{10^{p-2}}$.

"Log-noncorrelation"

That is, if the probability that two Theta-values are equal is $\frac{1}{10}$ and if there is *complete non-correlation* the probability that *all* $p-1$ *Theta-values are equal* would be $\frac{1}{10^{p-2}}$.

We don't need such full "non-correlation:' All we need is that the probability be no greater than something on the order of:

$$\frac{1}{10^{O(\log(p)}}.$$

It is this type of hypothesis, which we call

"Log-noncorrelation"

which we assume—together with our empirical data, plus belief in BSD—that gets Karl Rubin and me to conjecture the following:

Ranks of elliptic curves over Large abelian algebraic number fields

Conjecture: *Suppose* E *is an elliptic curve over* $\mathbb{Q}$*, and* $\mathsf{L} \subset \mathbb{Q}^{\mathrm{ab}}$ *is a real abelian field that contains only finitely many extensions of* $\mathbb{Q}$ *of degree* 2, 3, *or* 5. *Then* $E(\mathsf{L})$ *is finitely generated.*

For example, we can take the field L in this conjecture to be

- the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ for any prime p, in which case the conjecture is known to be true by work of Kato and Rohrlich. [In fact, any abelian extension of $\mathbb{Q}$ unramified outside finitely many primes.]

For example, we can take the field L in this conjecture to be

- the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ for any prime p, in which case the conjecture is known to be true by work of Kato and Rohrlich. [In fact, any abelian extension of $\mathbb{Q}$ unramified outside finitely many primes.]
- the compositum of all these $\mathbb{Z}_p$-extensions (i.e., for all p) in which case this was previously conjectured by Coates,

For example, we can take the field L in this conjecture to be

- the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ for any prime p, in which case the conjecture is known to be true by work of Kato and Rohrlich. [In fact, any abelian extension of $\mathbb{Q}$ unramified outside finitely many primes.]
- the compositum of all these $\mathbb{Z}_p$-extensions (i.e., for all p) in which case this was previously conjectured by Coates,
- the maximal abelian ℓ-extension of $\mathbb{Q}$ for any $\ell \geq 7$.

For example, we can take the field L in this conjecture to be

- the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ for any prime p, in which case the conjecture is known to be true by work of Kato and Rohrlich. [In fact, any abelian extension of $\mathbb{Q}$ unramified outside finitely many primes.]
- the compositum of all these $\mathbb{Z}_p$-extensions (i.e., for all p) in which case this was previously conjectured by Coates,
- the maximal abelian ℓ-extension of $\mathbb{Q}$ for any $\ell \geq 7$.
- the compositum of all of the above.

Hilbert's Tenth Problem over rings of algebraic integers

The original "Hilbert's Tenth Problem" was one of 23 problems posed over a century ago by David Hilbert in the ICM, at the Sorbonne, in Paris:

Problem

Is there an algorithm which when given an arbitrary polynomial equation in several variables over $\mathbb{Z}$*, answers the question of whether that equation has solutions in* $\mathbb{Z}$*?*

This question has been answered negatively

in the work of M. Davis, H. Putnam, J. Robinson and Yu. Matijasevich. Similar questions have been raised for other fields and rings: For what fields or rings of algebraic numbers does HTP have a negative answer?

Note: there is extensive literature on this, and all the references relevant to what I'm about to say are given in the paper in preparation: *Existential Definability and Diophantine Stability* (by Karl Rubin, Alexandra Shlapentokh and me).

This paper also contains the results we are about to discuss.

Diophantine definitions of rings of integers

Let L/K be an extension of number fields.
Suppose given a set of m polynomial equations in $n+1$ variables with coefficients in $\mathcal{O}_K$:

$$\mathcal{F} := \quad \{F_i(\mathrm{t}, x_1, x_2, \ldots, x_n)\} \text{ for } i = 1, 2, \ldots, m$$

where we have 'singled out' the variable t.

Say that $\mathcal{F}$ provides a diophantine definition of $\mathcal{O}_K$ in $\mathcal{O}_L$ if

1. Every simultaneous solution of the equations

$$F_i(\mathrm{t}, x_1, x_2, \ldots, x_n) = 0; i = 1, 2, \ldots, m$$

   where t and all the x_i take values in $\mathcal{O}_L$, the variable t takes its value in $\mathcal{O}_K$, and

2. *Every* element of $\mathcal{O}_K$ occurs as such a value (of t).

Diophantine definitions of rings of integers for people who like schemes:

The same definition:

Let L/K be an extension of number fields, and:

$$V := \mathrm{Spec}\ (\mathcal{O}_K[\mathtt{t}; x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m))$$

Let $\mathrm{Aff}^1 = \mathrm{Spec}\ (\mathcal{O}_K[\mathtt{t}])$ be 1-dimensional affine space, viewed as (an affine) scheme over $\mathcal{O}_K$.

The natural homomorphism:

$$\mathcal{O}_K[\mathrm{t}] \longrightarrow \left\{\mathcal{O}_K[\mathtt{t}; x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_m)\right\}$$

induced by sending $\mathrm{t} \mapsto \mathtt{t}$ can be viewed as an $\mathcal{O}_K$-morphism:

$$V \xrightarrow{\mathrm{t}} \mathrm{Aff}^1$$

which in turn induces a map on $\mathcal{O}_L$-valued points

$$V(\mathcal{O}_L) \longrightarrow \mathcal{O}_L.$$

Diophantine definitions of rings of integers

This morphism of affine schemes:

$$V \xrightarrow{\mathrm{t}} \mathrm{Aff}^1$$

will be called a **Diophantine definition of $\mathcal{O}_K$ in $\mathcal{O}_L$** if the image of $V(\mathcal{O}_L) \longrightarrow \mathcal{O}_L$ is precisely

$$\mathcal{O}_K \subset \mathcal{O}_L.$$

The Category of all Diophantine definitions of $\mathcal{O}_K$ in $\mathcal{O}_L$

There are loads of open questions worth examining about the category of diophantine definitions related to number field extensions!

The Category of all Diophantine definitions of $\mathcal{O}_K$ in $\mathcal{O}_L$

There are loads of open questions worth examining about the category of diophantine definitions related to number field extensions!

(E.g., given the existence of a Diophantine definition, what is the affine scheme of smallest dimension providing a Diophantine definition of $\mathcal{O}_K$ in $\mathcal{O}_L$?)

Diophantine definitions and HTP

Let L/K be an extension of number fields. If

- HTP has a negative answer for $\mathcal{O}_K$ the ring of integers in K

and if

- there is a diophantine definition of $\mathcal{O}_K$ in $\mathcal{O}_L$,

then

- HTP has a negative answer for $\mathcal{O}_L$.

Bootstrap up:

Since HTP has a negative answer for Z (thanks to Yuri Matiyasevich, Martin Davis, et al)

—we can try to show that HTP has a negative answer for the ring of integers in any number field, by finding

—maybe—

diophantine definitions of $\mathcal{O}_K$ in $\mathcal{O}_L$ for every number field extension.

Bootstrapping up to any totally real number field!

(J. Denef, L. Lipshitz, Diophantine Sets over Some Rings of Algebraic Integers Journal of the London Mathematical Society, **18** 1978 (385-391))

Recall that a "number field,' means a field of *finite degree* over Q. We'll get to **large** algebraic numbers fields—i.e., fields of algebraic numbers of infinite degree later.

Theorem

The ring of (rational) integers has a Diophantine definition in the ring of integers in any totally real number field.

Corollary

HTP has a negative answer any totally real number field L.

Say a word about the method of proof—making use of unit equations in quadratic extensions of L; and its connection with a similar argument of Martin Davis...

Transporting diophantine definitions of rings of integers

(Using work of Cornelissen-Pheidas-Zahidi, Poonen, Shlapentokh.)

Let $K \subset L$ be number fields. If there exists an elliptic curve E over K having **(a)** infinitely many rational points over K

and

(b) the diophantine-stability property for the extension L/K:

$$E(K) = E(L).$$

Then there is a diophantine definition of $\mathcal{O}_K$ in $\mathcal{O}_L$.

Abelian varieties, more generally

Sasha, Karl and I recently proved, more generally:

Theorem

Let L/K be a number field extension with $\mathcal{O}_L/\mathcal{O}_K$ the corresponding extension of their rings of integers. Let A be an abelian variety defined over K such that
$\mathrm{rank}\ \mathrm{A(L)} = \mathrm{rank}\ \mathrm{A(K)} \geq 1.$

Then $\mathcal{O}_K$ has a diophantine definition over $\mathcal{O}_L$. Further, if L is a totally real field or a quadratic extension of a totally real field, this diophantine definition can be made uniform in the degree of L over $\mathbb{Q}$.

Diophantine definitions and Diophantine Stability

Mention: this generalizes to arbitrary smooth group schemes over rings of integers.

And mention the query about whether diophantine stability can (or must?) always take a role in any diophantine definition of the rings of integers within number field extensions.

Diophantine Stability for Large fields

Is $\mathcal{O}_{\mathrm{Q}^{\mathrm{ab}}} = \mathrm{Z}[\mu]$ diophantine undecidable?

Here is what our heuristic gets us to conjecture:

Suppose our conjecture holds. Let $p = 7$ or 11. Then we construct:

- a real abelian field L with $[\mathrm{Q}^{\mathrm{ab}+} : \mathrm{L}] = p$, and
- an abelian variety A/Q such that $\mathrm{rank}\ A(\mathrm{Q}) > 0$ and $A(\mathrm{L})$ is finitely generated.

If the Birch and Swinnerton-Dyer conjecture holds for elliptic curves, then the same statement holds for $p = 13$.

It will follow from our heuristic, then, (plus standard conjectures) that—

for all such fields L, the ring Z has a diophantine definition in $\mathcal{O}_\mathrm{L}$ and therefore $\mathcal{O}_\mathrm{L}$ is diophantine undecidable.

What about $\mathcal{O}_{\mathbb{Q}^{\mathrm{ab}}}$ itself?

We're at some sort of border here in the sense that we don't even have a 'heuristic' to nudge us to guess whether or not $\mathcal{O}_{\mathbb{Q}^{\mathrm{ab}}}$ is diophantine undecidable—

Note that elliptic curves, at least, can't play much of a role in a diophantine definition of Z in $\mathcal{O}_{\mathbb{Q}^{\mathrm{ab}}}$

What about $\mathcal{O}_{\mathbb{Q}^{ab}}$ itself?

We're at some sort of border here in the sense that we don't even have a 'heuristic' to nudge us to guess whether or not $\mathcal{O}_{\mathbb{Q}^{ab}}$ is diophantine undecidable—

Note that elliptic curves, at least, can't play much of a role in a diophantine definition of Z in $\mathcal{O}_{\mathbb{Q}^{ab}}$

Thanks for listening, and...

I hope I've left enough time for Nati Linial and Yuval Peled to present their data for the neat statistical and 'non-correlational heuristic' problem they are currently working on.