Hilbert's classical Tenth Problem

Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients:

To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

Successes, Non-successes

Nowadays one has a large number of different *processes* in our experience (i.e., *successes*).

From algorithms to find the maxima of functions on convex polytopes (e.g.: Linear programming)

to procedures for factoring numbers into product of primes.

The basic questions we tend to ask about these have to do with running time.

Non-successes

We also have quite a number of guaranteed non-successes:

- There is no finite algorithm to determine, given a finite presentation of a group, whether or not the group is trivial. Or whether two finite presentations present isomorphic groups.
- The *recognition problem for manifolds in dimension four or higher* is unsolvable (it being related directly to the recognition problem for finitely presented groups).

Infinite versus Finite

And even when one looks for interesting Diophantine examples, they often come in formats somewhat different from the way Hilbert's Problem is posed. For example,

sometimes we're interested in procedures to determine whether any given polynomial equation over the rational field $\mathbf{Q}$ has *finitely many* or *infinitely many* solutions.

Infinite versus Finite

And even when one looks for interesting Diophantine examples, they often come in formats somewhat different from the way Hilbert's Problem is posed. For example,

sometimes we're interested in procedures to determine whether any given polynomial equation over the rational field $\mathbf{Q}$ has *finitely many* or *infinitely many* solutions.

But: *finitely many* $\leftrightarrow$ *infinitely many*

is not a distinction that Hilbert formulates.

Families

And, often, we're interested not in answering the yes-or-no question about rational solutions for any single polynomial equation but, rather for whole families of them.

Families

And, often, we're interested not in answering the yes-or-no question about rational solutions for any single polynomial equation but, rather for whole families of them.

For example, the *congruent number problem* is the problem of determining those rational numbers r that can be expressed as the area of a right triangle with three rational number sides.

$$6, 15, 30, 210, 210, 21, 126, 70, 5, \ldots$$

This turns out to be *equivalent* to asking that the equation

$$y^2 = x^3 - r^2 x$$

have a rational solution with $y \neq 0$.

Back to Hilbert

So you might ask why—except for historical reasons—might one be interested in pursuing the question as Hilbert posed it?

One answer (which is already enough to spark interest!) is that it is a problem that has led to great developments in the intersection of mathematical logic and number theory.

But also, Hilbert's Problem calls for the answers to new *kinds of* questions in number theory, and specifically in the arithmetic of elliptic curves.

The Program for these lectures

(1) Hilbert's Tenth Problem and Diophantine Stability

(2) Elliptic Curves and their rational points

(3) Methods

Solving polynomial equations over finitely generated rings

Hilbert Problem for A

Given an infinite, but finitely generated, commutative ring A is there an algorithm to determine—in finite time—whether a polynomial in finitely many variables with coefficients in A has a solution or not?

INPUT $\Longrightarrow$ OUTPUT

INPUT: A finite collection of polynomial equations

$$f_i(X_1, X_2, X_3, \ldots, X_n)$$

with coefficients in A.

INPUT $\Longrightarrow$ OUTPUT

INPUT: A finite collection of polynomial equations

$$f_i(X_1, X_2, X_3, \ldots, X_n)$$

with coefficients in A.

OUTPUT: "Yes," or "'No," answering the question of whether or not there is an n-tuple of elements of A $(a_1, a_2, a_3, \ldots, a_n)$ such that

$$f_i(a_1, a_2, a_3, \ldots, a_n) = 0$$

for all i.

Solving polynomial equations over finitely generated rings

Immense amount of classical work on precursors to, and variants and extensions of such problems.

J. Robinson, M. Davis, H. Putnam, Y. Matiyasevich

as well as more recent work of

J. Denef,
G. Cornelissen, T. Pheidas, and K. Zahidi,
B. Poonen,
A. Shlapentokh,
J. Koenigsmann,
K. Eisentrager,
J. Park

A conditional solution

Karl Rubin and I did some work on Hilbert's problem for a general finitely generated (infinite) commutative ring. We didn't answer that question unconditionally, but rather we proved a theorem—that we like to think of as a

Diophantine Stability Result

having to do with the arithmetic of elliptic curves that, when coupled with a standard conjecture in the arithmetic of elliptic curves, gave what was needed to offer a negative answer to Hilbert's problem for any infinite, but finitely generated, commutative ring A.

Dependent, of course, on that prior work.

Diophantine Stability Issues

Call the stability property that enters in this discussion '**diophantine-stability:**

Let L/K be a field extension, and

$$P(X_1, X_2, \ldots, X_n)$$

a polynomial with coefficients in K (or more generally a system of such polynomials).

Diophantine Stability Issues

Call the stability property that enters in this discussion '**diophantine-stability:**

Let L/K be a field extension, and

$$P(X_1, X_2, \ldots, X_n)$$

a polynomial with coefficients in K (or more generally a system of such polynomials).

Say that the polynomial P is **diophantine-stable** for the extension L/K if P acquires no *new* zeroes over L.

Diophantine Stability and Hilbert's Tenth Problem

To transport *undecidability* from the ring of integers of one field to the ring of integers of a larger ring one uses the existence of elliptic curves containing rational points of infinite order over a given number field K having sufficient diophantine stability.

the Bootstrap Method

The classical work of Matiyasevich

There is no algorithm for the ring $A = \mathbf{Z}$.

To say that there is no such algorithm is by no means a completely *negative* statement, given the format of Matiyasevich's proof.

The classical work of Matiyasevich

- For Matiyasevich uses the known fact that there are subsets S of the integers that are undecidable in the simple sense that although:
  - there may be an algorithm to list the elements of S,
  - there is no algorithm to list the elements of the complement of S in $\mathbf{Z}$, so we don't have a way of computing whether or not a given integer is in S;

  and

- he is able to define *any such* S by a diophantine method.

The classical work of Matiyasevich

That is, diophantine formulations capture all listable sets (including the "undecidable ones"). Diophantine vocabulary is very rich!

E.g., do you want a polynomial over $\mathbf{Z}$ whose set of positive values is the set of *exactly all* prime numbers for integral substitution of all its 26 variables?

Here is one:

(this is due to J. Jones, D. Sato, H. Wada and D. Wiens)

Prime Numbers

$$(k+2)\{1-[wz+h+jq]^2-[(gk+2g+k+1)(h+j)+hz]^2-[2n+p+q+ze]^2[16(k+1)^3(k+2)(n+1)^2+1f^2]^2-[e^3(e+2)(a+1)^2+1o^2]^2-[(a^21)y^2+1-x^2]^2x-[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2-[n+l+vy]^2-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}$$

Listable versus Diophantine

One standard way of refining Hilbert's question is to "reset" it as a problem related to *listable* sets and *Diophantine sets*, as hinted at in the example of primes.

Listable sets of integers

(synonyms: *recursively enumerable*, *computably enumerable*)

Listable

A subset $\mathcal{L} \subset \mathbf{Z}$ is called **listable** if there exists a finite computer program whose output gives a sequence $\alpha_1, \alpha_2, \alpha_3, \ldots$ of integers such that the set $\mathcal{L}$ is precisely this collection of numbers; i.e.,

$$\mathcal{L} = \{\alpha_1, \alpha_2, \alpha_3 \ldots\}.$$

A computer algorithm that does job this will be called a computer algorithm that "lists $\mathcal{L}$."

Easily versus not so easily listable

Note, though, that–even if the computer spits out a "new" integer every second— the ordering in which the integers in $\mathcal{L}$ come via the computer's list may be helter-skelter in terms of absolute values.

If you suspect that a given number, say 2, is *not* in $\mathcal{L}$ and need to have a definite guarantee of the truth of your suspicion, well . . .

running the helter-skelter computer algorithm for any finite length of time may be of no help to you.

Easily listable

A more useful finite computer program might be, for example, a program that for each integer N will, after some guaranteed time

(e.g., no greater than $N^{N^{\cdots^N}}$ hours)

actually produces a *complete* list of *all* integers of absolute value $\leq N$ that are in $\mathcal{L}$.

(Call such a program a *deluxe program*.)

Moderately easily listable

Somewhat intermediary to the above two types of computer programs (helter-skelter, and deluxe) would be a *pair* of computer programs,

one of which spits out the elements of $\mathcal{L}$ and

the other spits of the elements of the complement of $\mathcal{L}$.

Supplied with such a pair of programs you might, at the very least:

- run the first program by day,
- and the second by night,

for then you are guaranteed to know—in some (perhaps unspecified, but) finite time whether or not 2 is in your set $\mathcal{L}$.

Recursive

A set $\mathcal{L}$ that has the property that it and its complement are both listable is called *recursive*.

If you have such a recursive set, then, as mentioned—listing the set $\mathcal{L}$ by day and its complement $\mathbf{N} - \mathcal{L}$ by night—you are guaranteed that for every $N \in \mathbf{N}$ you will know at some finite time whether or not N is in your set.

Alan Turing

There exist listable sets that are *not* recursive. (The computer algorithms that list such sets are necessarily quite helter-skelter!)

This is a consequence of the famous 1936 theorem of Alan Turing that was phrased in terms of

The halting problem for algorithms.

Turing showed that there exists no universal algorithm to tell you whether or not any finite computer algorithm will terminate finitely, when run.

The Halting Set

$$\mathbf{H} := \{\text{The set of couples } (P, x)$$

where P is a program and

x is a possible input to program P and

such that *Program* P will eventually *halt*

if run with input $x\}$

Variants of Hilbert's Problem

Hilbert's Problem for the field $\mathbf{Q}$?

More generally for subfields in $\bar{\mathbf{Q}}$?

For 'big' subfields of $\bar{\mathbf{Q}}$?
Real algebraic numbers, p-adic algebraic numbers,...

For polynomials of degree three in many variables over $\mathbf{Z}$?

First-order undecidability?

First-order undecidability?

A **Diophantine question** asks simply whether a quantity (or quantities) $\exists$ satisfying a diophantine relation.

A **First-order question** may ask—for example— whether or not a quantity exists satisfying a specific relation to *any* quantity that satisfies some diophantine relation. $\forall\exists$? And so on, like:

$$\forall W \exists X \forall Y \exists Z \text{ such that } f(W, X, Y, Z) = 0?$$

Gödel (1931)

Incompleteness Theorem $\Longrightarrow$ There is no algorithm to decide first-order questions about $\mathbf{Z}$.

Julia Robinson: None to decide first-order questions about $\mathbf{Q}$ or number fields, or rings of integers in number fields.

Bootstrap to $\mathbf{Z}$*:*

If you can find a first-order formula that defines the ring $\mathbf{Z}$ in a larger ring A, Matiyasevich's Theorem then also shows there is no algorithm to decide first-order questions about A.

The fun of "first-order definitions" of **Z** in **Q**

Classical work of Julia Robinson,

Recent work of Joechen Koenigsmann, Bjorn Poonen, Jennifer Park, G. Cornelissen, K. Zahidi

Bjorn Poonen's first order definition of **Z** in **Q**:

A rational number t is an integer if for all pairs of rational numbers a, b there are seven rational numbers

$$x_1, x_2, \ldots, x_7$$

such that

$$(a+\sum_{i=1}^{4} x_i^2)\cdot(b+\sum_{i=1}^{4} x_i^2)\cdot(x_1^2-ax_2^2-bx_3^2+abx_4^2-1)^2=$$

$$=\ -\prod_{n=0}^{2309}((n-t-2x_1)^2-4ax_5^2-4bx_6^2-4abx_7^2-4)^2.$$

Undecidablity versus Decidability for big rings

- First-order problems undecidable over number fields or over their rings of integers.
- R. Rumely (1986): Hilbert's Tenth Problem is decidable over the ring of all algebraic integers.
- Van de Dries: First-order Theory is decidable over the ring of all algebraic integers.
- A. Prestel, J.Schmid, J.(1991): First-order problems are decidable for the ring of real algebraic integers, and—for any p—for the ring of algebraic integers in the p-adics.

First-order undecidability in large fields of algebraic numbers

Using results of Alexandra Shlapentokh (and prior work cited) Karl Rubin and I prove (via some Diophantine-stability results):

Theorem: Let p be any prime number (or ∞).

There are uncountably many subfields K of the field of algebraic numbers in $\mathbf{Q}_p$ in which:

*there is a *first order definition* of* $\mathbf{Z}$ *in* K*.*

(The first-order theory for any such field K—and for its ring of algebraic numbers—is undecidable.)

Diophantine stability in a more general context

Fix a variety V over, say, a number field K. Is there a nontrivial field extension L/K for which it is diophantine-stable?

Rational curves defined over K

If $V = \mathbf{P}^1$ over the field K (or any nonempty open piece of $\mathbf{P}^1$) the answer is no.

$\mathbf{P}^1$ has new points in every nontrivial extension L/K.

More generally:

If there is a curve in V that is isomorphic to an open subvariety of the projective line over K the answer is clearly no.

Is this the only obstruction to a positive answer to the above question?

A characterization of $\mathbf{P}^1$?

Question:

If V is a projective variety over a number field K such that for every nontrivial number field extension L/K there are new points, i.e.,

if for all L/K the set $V(L)$, of points of V rational over the field L is strictly larger than $V(K)$,

does V necessarily contain the image (under a nonconstant mapping defined over K) of the projective line over K?

When V is a curve

Karl Rubin and I (with help from Michael Larson) have recently proved that if V is a curve the answer to this question is yes.

To formulate this more precisely:

Field extensions 'belonging to" a variety

Let K be a number field and V an irreducible algebraic variety over K.
If V is a variety over K say that

$$L/K \textbf{ belongs to } V \textbf{ over } K$$

if L is generated over K by (the coordinates of) a single point of V.

For example: any elliptic curve $y^2 = x^3 + ax + b$ over $\mathbf{Q}$ has infinitely many quadratic fields belonging to it.

The collection of fields belonging to a variety

Denote by $\mathcal{L}(V;K)$ the set of field extensions of K belonging to V. That is:

$$\mathcal{L}(V;K) := \{K(x)/K \ ; \text{for } x \in V(\bar{\mathbf{Q}})\}.$$

Working both sides

Fix a variety V and study extensions L/K belonging to it.

Fix an extension L/K and study varieties to which it belongs.

Two Diophantine Stability results for elliptic curves (and abelian varieties)

Karl Rubin and I showed:

Theorem

Let K be a number field.

(1) *Let E be an elliptic curve over K with no CM, and n be a positive integer. There are infinitely many primes ℓ where, for each of them, there are infinitely many cyclic extension fields L/K of degree ℓ^n such that*

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

Theorem

(2) *Let L/K be a cyclic extension of prime degree. Then conditional on the 2-Shafarevich-Tate Conjecture there exists an elliptic curve over K such that $E(K)$ is an infinite cyclic group and $E(K) = E(L)$.*

Diophantine stability for curves of positive genus

(Using a result of Michael Larsen) we show that for any curve of positive genus there are many extension fields do not belong to it:

Theorem

Beamer

(3) *Let X be an irreducible nonsingular projective curve over a number field K not of genus 0. Then there is a finite extension K'/K such that for any positive integer n,*

- *there are infinitely many primes ℓ where, for each of them,*
- *there are infinitely many cyclic extension fields L/K' of degree ℓ^n such that $X(K') = X(L)$.*

We show this by relating curves to (absolutely simple) abelian varieties, via their jacobians.

a statistical question

Fixing a curve X of positive genus over a number field K, is it the case that for any prime number

$$\ell \gg_{X,K} 0$$

100% of the cyclic degree ℓ extensions L/K have the property that $X(K) = X(L)$?

Minimalist View

. . . that—all in all–rational points are rare and when they come in profusion they do so for some eventually graspable reason, and not because they happen.

I'll be discussing this phenomenon in these lectures, reviewing aspects of the logical vocabulary we used, the basics of elliptic curves, and the various tools for examining aspects of the problem; specifically Selmer groups over arbitrary number fields.

Statistics for elliptic curves over $\mathbf{Q}$

Chantal David, Jack Fearnley and Hershy Kisilevsky conjecture:

For a fixed elliptic curve over $\mathbf{Q}$ and $\ell \geq 7$, there are only finitely many non-diophantine-stable cyclic extensions of $\mathbf{Q}$ of degree ℓ. (??)

For $\ell = 3$ and 5, following random matrix heuristics, they make (essentially) these statistical conjectures:

Statistics for elliptic curves over $\mathbf{Q}$

For E and elliptic curve over $\mathbf{Q}$, let

$$N_{E,\ell}(X)$$

be the number of cyclic extensions L/K of degree ℓ *belonging the* E *over* $\mathbf{Q}$ that are cut out by a Dirichlet character (of order ℓ and) of conductor $\leq X$.

They conjecture that:

$$\log N_{E,3}(X) \sim \frac{1}{2}\log(X),$$
$$\log N_{E,5}(X) <<_{\epsilon} X^{\epsilon}.$$

A related topic: Statistics for modular symbols of elliptic curves

(*with Karl Rubin and William Stein*)

Let E be an elliptic curve over $\mathbf{Q}$ with L-function

$$L(e,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

and with

$$[\frac{a}{N}]_E$$

the "real" modular symbol attached to E.

Modular symbols don't look random

Fixing $N = p$ a large prime, form the function for $0 \leq \tau \leq 1/2$,

$$G_{E,p}(\tau) = \sum_{0 \leq \frac{a}{p} \leq \tau} [\frac{a}{p}]_E.$$

(The integral of the step-function determined by the modular symbols.)

Approximating $G_{E,p}(\tau)$

It is natural to try to compare $G_{E,p}(\tau)$ with the (convergent) function:

$$g_E(\tau) \;=\; \sum_{n=1}^{\infty} \frac{a_n}{n^2} \sin(2\pi i n\tau)/2\pi$$

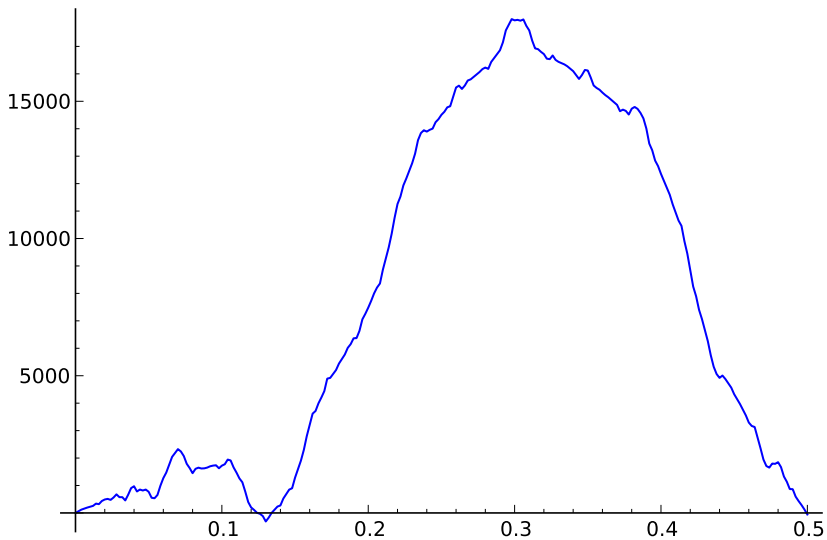
Specifically, we conjecture:

$$\lim_{p\to\infty} G_{E,p}(\tau) \;\stackrel{??}{=}\; g_E(\tau).$$

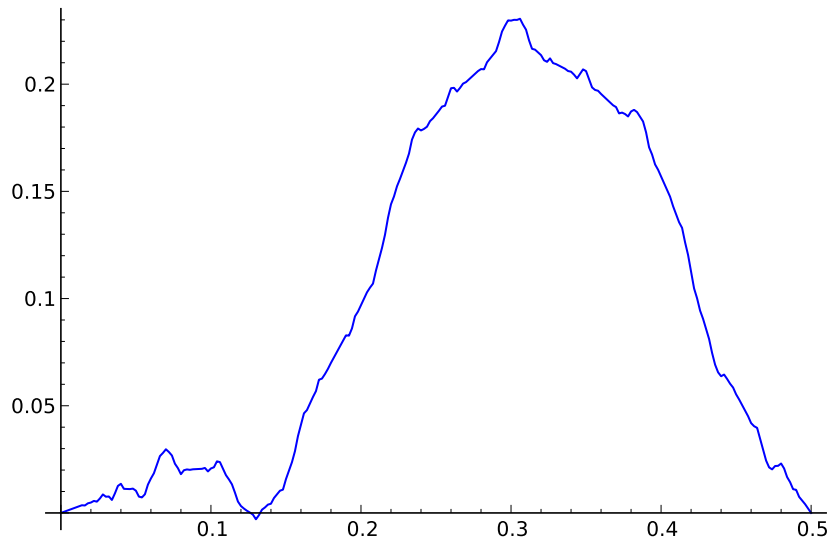
Some data

$E = 11a; \quad p = 100,003$

$G_{E,p}$

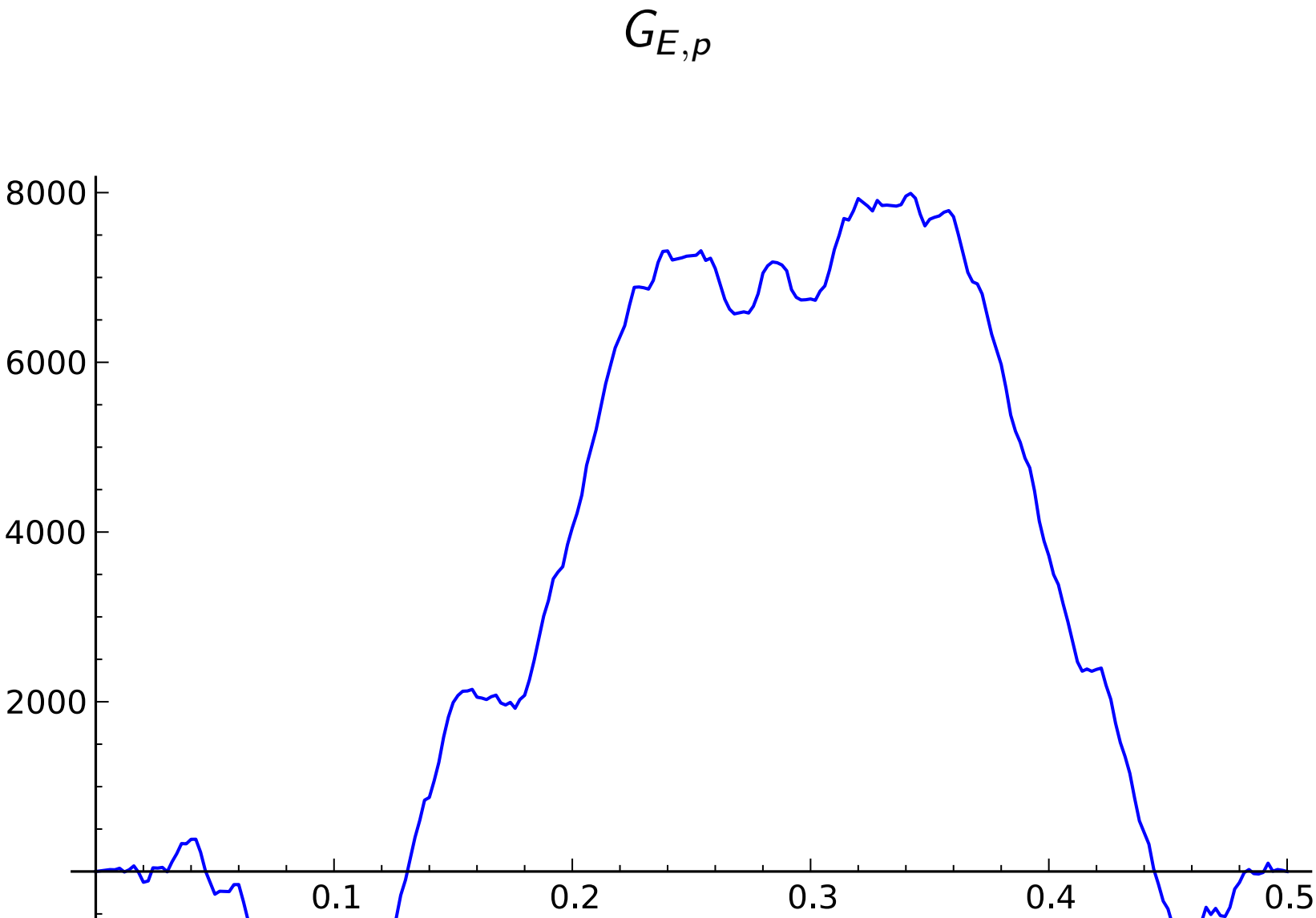


g_E



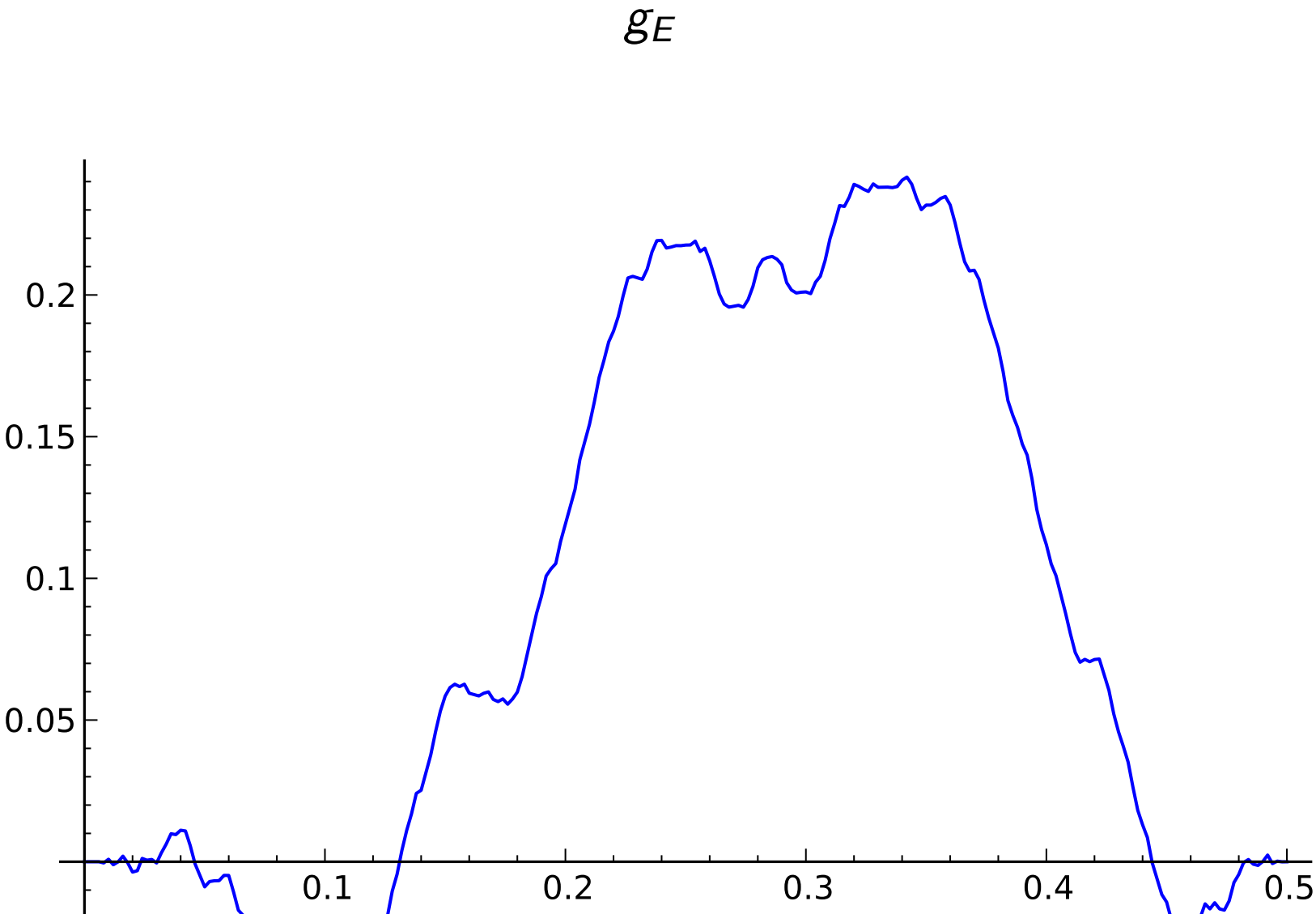
Some data

$E = 37a; \quad p = 100,019$



Some data

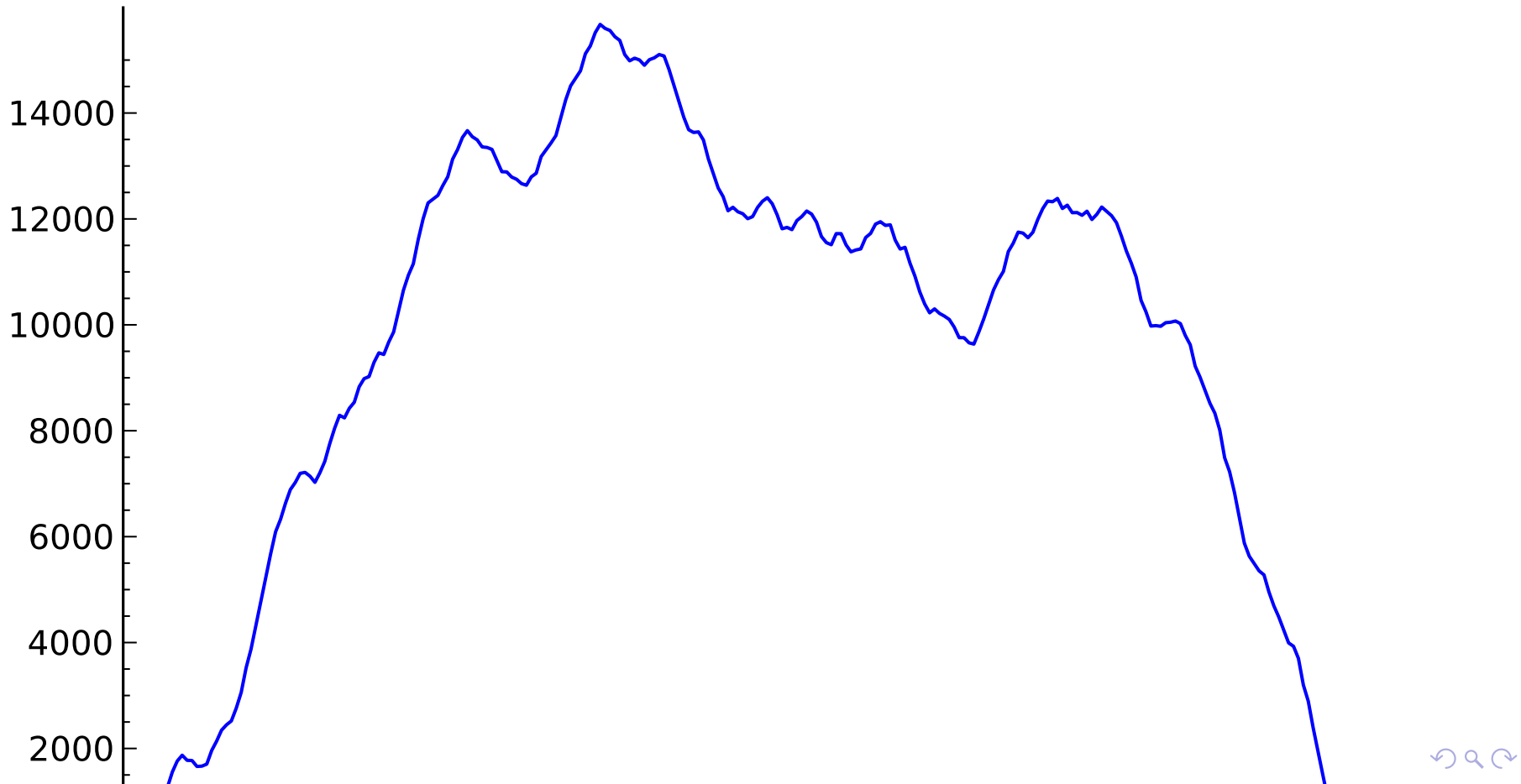
$E = 37a; \quad p = 100,019$



Some data

$E = 37b; \quad p = 100,043$

$G_{E,p}$



Some data

$E = 37b; \quad p = 100,043$