

Hilbert's Tenth Problem



Write down a random polynomial equation in two or more variables with coefficients in the ring of integers, e.g.,

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

and—chances are— it will be very tricky to find all its solutions; often you will be quite challenged by the question of whether or not it *has* solutions.

Hilbert spurred mathematicians to systematically investigate the general question:

How solvable are such diophantine equations?

I will talk about this, and its relevance to specific number theoretic projects, and then aim towards some recent work, joint with Karl Rubin.

Here is a close translation of Hilbert's formulation of the 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.

- *a Diophantine equation*
- *process*

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.

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).

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,

- we have a (deep) decision procedure to determine whether any given elliptic curve over the rational field \mathbf{Q} has *finitely many* or *infinitely many* solutions. But this distinction

$$\textit{finitely many} \leftrightarrow \textit{infinitely many}$$

is not a distinction that Hilbert formulates.

- And, sometimes, we're interested not in answering this question for any single elliptic curve but, for whole families of them.

For example, the *congruent number problem* is the problem of determining those positive integers n that can be expressed as the area of a right triangle with three rational number sides. This turns out to be *equivalent* to asking that the elliptic curve

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

have infinitely many rational points.

- And, we sometimes try to find single processes that work even allowing for variation of the exponents involved.

As in:

1. *Catalan-type Problems*

For a given integer k find all *perfect powers* that differ by k .

$$Y^n - X^m = k$$

Example: *the only two consecutive perfect powers are:*

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

or as in:

2. *Fermat's Last Theorem.*

So you might ask why—except for historical reasons—might one be interested in pursuing the question as Hilbert posed it. The answer (which is already enough to spark my interest) is that it is a problem that has led to the most magnificent developments in mathematical logic, and in the intersection of mathematical logic and number theory.

But also, thanks to relatively recent work (of Denef, Denef-Lipschitz, Pheidas, Shalapentokh and Poonen) Hilbert's Problem calls for the answers to new *kinds of* questions in number theory, and specifically in the arithmetic of elliptic curves.

So, back to Hilbert's Tenth Problem!

Hilbert is particular in the type of solutions (rational integers) he seeks. Nevertheless, in considering “Hilbert’s 10th Problem” we often specifically interpret *Diophantine equation, process* and sometimes generalize the type of solutions being considered. We then end up with a question roughly of the following form:

Let A be a commutative ring. Does there exist a finite algorithm to determine whether any finite system of polynomial equations in finitely many variables with coefficients in A has a solution in A or not?

INPUT: A finite collection of polynomial equations

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

with integer coefficients.

OUTPUT: “Yes,” or “No,” answering the question of whether or not there is an n -tuple of integers $(a_1, a_2, a_3, \dots, a_n)$ such that

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

for all i .

One standard way of refining the above question is to “reset” it as a problem related to *listable* sets and *Diophantine sets*.

Listable sets of integers

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

I’ll start with some examples of sets that are easy to “list”



$2, 3, 5, 7, 11, 13, 17, 19, 23, \dots$



$2!, 3!, 4!, 5!, \dots$

Discuss what is meant by *easy*

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

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

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

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. Therefore 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 (... if you are right!) running the helter-skelter computer algorithm for any finite length of time will be of no help to you.

- 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 $N^{N \dots N}$ 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*.)

- 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 out 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 sets

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.

The Halting Problem

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.

More specifically, the so-called *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 }

is listable—once you code, in a computable way, the (P, x) 's as a subset of natural numbers—BUT the *complement* of this set is not listable.

Diophantine sets

Roughly, a *Diophantine subset* of integers (or of natural numbers) is a subset that can be defined using the *seemingly very restricted* vocabulary of polynomials.

Here is one way of formulating this concept over a fairly general ring.

Let A be a commutative noetherian integral domain, the main example being $A = \mathbf{Z}$.

Definition: Let $\mathcal{D} \subset A$ be a subset of the ring A .

Say that \mathcal{D} is **Diophantine in A** if there exists a finite set of polynomials with coefficients in A , in finitely many variables

$$f_i(T; X_1, X_2, \dots, X_n) \in A[T, X_1, X_2, \dots, X_n]$$
$$(i = 1, 2, \dots, m)$$

such that for $\alpha \in A$ the system of polynomial equations

$$f_i(\alpha; X_1, X_2, \dots, X_n) = 0$$

has a simultaneous solution

$$(X_1, X_2, \dots, X_n) = (a_1, a_2, \dots, a_n) \in A^n$$

if and only if

$$\alpha \in \mathcal{D} \subset A.$$

If this happens say that the set of polynomials **cut out** \mathcal{D} .

Notice the evident proposition:

Proposition: If $A = \mathbf{Z}$ (or, more, generally, a countable ring) and $\mathcal{D} \subset A$ is Diophantine, then \mathcal{D} is listable.

Moreover, any set of polynomials

$$\{f_i(\alpha; X_1, X_2, \dots, X_n)\}_i$$

(for $i = 1, 2, \dots, m$) that “cut out” \mathcal{L} leads to a computer algorithm that lists \mathcal{L} .

Remarks:

(1) The collection of Diophantine subsets of an integral domain A is closed under finite union and intersection.

Proof: It suffices to do this for two Diophantine sets $D, E \subset A$:

Let the systems of polynomials

$$\{f_i(t; X_1, \dots)\}_i$$

and

$$\{g_j(t; Y_1, \dots)\}_j$$

cut out D and E respectively.

- The “union” of the two systems, (viewed as polynomials in t and the independent variables X_μ and Y_ν) cuts out $D \cap E$.

- The “product” system given by

$$\{f_i(t; X_1, \dots) \cdot g_j(t; Y_1, \dots)\}_{i,j}$$

cuts out $D \cup E$.

Diophantine sets are closed, as well, under polynomial mappings.

Mention: scheme-theoretic definition

(3) For us the most important ring is $A = \mathbf{Z}$. In this context you can replace any finite system of polynomials $\{f_i(t; X_1, \dots)\}_i$ that “cut out” a set D by a single polynomial

$$\sum_i f_i(t; X_1, \dots)^2.$$

One is now faced with the task of building a Diophantine vocabulary.

Here is a list of subsets of \mathbf{Z} that are Diophantine (and easily proven to be).

1. Lagrange's Theorem says that any positive whole number is expressible as a sum of four squares.

E.g

$$401 = (20)^2 + 1^2 + 0^2 + 0^2$$

well ... that might have been too easy an example ...

In our Diophantine vocabulary, this means that the polynomial

$$f(t; X_1, X_2, X_3, X_4) := t - \sum_{i=1}^4 X_i^2$$

cuts out the set of positive integers; so the set of positive numbers is Diophantine.

2. Therefore it follows, by easy steps, that these sets are too:

- the set of numbers $\geq a$ for any given $a \in \mathbf{Z}$,
- the set of numbers $\leq b$ for any given $b \in \mathbf{Z}$,
- any finite subset of \mathbf{Z} ,
- the complement of any finite subset of \mathbf{Z} .

3. So, if D is Diophantine, then any set obtained from D by removing and adding finite sets is also Diophantine.
4. Arithmetic progressions are Diophantine; as are the set of all squares, all cubes, all n -th powers for any given n .
5. Composite numbers.
6. For any fixed (say, nonsquare, positive) integer d , consider the set of integers t that come in solutions of the Pell equation

$$t^2 - ds^2 = 1$$

(this being a set that grows roughly exponentially).

The evolution of Hilbert's problem as developed through the work of

Martin Davis
Julia Robinson
Hillary Putnam
Yuri Matiyasevich:

The culminating theorem is due to Matiyasevich:

Theorem Every listable subset of \mathbf{Z} is Diophantine.

Thus *listable* and *Diophantine* are equivalent conditions for subsets of \mathbf{Z} .

Since there exist listable subsets of \mathbf{Z} that are not recursive—i.e., such that their complements are *not listable*, Matiyasevich's Theorem gives a negative answer to Hilbert's question above, but does far more than just that.

For example:

1. It certainly shows that there are systems of polynomials over \mathbf{Z} that admit no “deluxe computer program” as described.
2. The result also implies that relatively benign subsets of \mathbf{Z} can be Diophantinely described, as well. This is not as clear as one might think even for the most familiar subsets. For example:

- There is a system of polynomials that cut out the set of factorials $1!, 2!, 3! \dots$. The fact that this set is Diophantine played a big role in the development of the subject.

By the way, to get such a polynomial one starts by finding a Diophantine way of expressing the binomial coefficients $\binom{n}{m}$ and then dealing with the—to me surprisingly unpromising—formula

$$m! = \lim_{n \rightarrow \infty} \frac{n^m}{\binom{n}{m}}.$$

(!!!)

The *factorial* operation has quite a powerful effect if one allows it to be used as a piece of equipment to generate recursively enumerable sets. For example, the set of numbers $\alpha > 1$ such that the expression

$$\alpha \cdot X_1 + (\alpha - 1)! \cdot X_2 = 1$$

has a zero for integers X_1, X_2 is precisely the set of prime numbers. But regarding prime numbers, more relevant for our story is the fact that...

- There is a polynomial over \mathbf{Z} whose set of positive values is the set of *exactly all* prime numbers for integral substitution of its variables. A specific such polynomial is given by [**JSWW76**]:

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

Comments on the History

For a historical (and basic mathematical) account of this work it would be difficult, I think, to do better than the very informative wikipedia entry on *Hilbert's tenth Problem* which has a chart listing work ranging from 1944 when Emil Post said that Hilbert's tenth problem "begs for an unsolvability proof" to 1970 when Matijasevic clinched the theorem.

On the way to the final formulation of the theorem there is Martin Davis's formulation of what I'll, for reference, call **Davis Sets**.

Definition: A **Davis Set** is a set of natural numbers Δ such that there exists a polynomial with integral coefficients

$$P(T, K, Y, X_1, X_2, \dots, X_n)$$

in independent variables

$$T, K, Y, X_1, X_2, \dots, X_n$$

for some n , such that $a \in \mathcal{A}$ if and only if there is a nonnegative integer y such that for all nonnegative integers $k < y$ the polynomial

$$P(a, k, y, X_1, X_2, \dots, X_n)$$

has a solution in natural numbers

$$X_1 = a_1, X_2 = a_2, \dots, X_n = a_n.$$

Now *Davis sets* are fairly clearly recursively enumerable. In 1949 Davis proved the converse: that every recursively enumerable subset of the set of natural numbers has the above form; i.e., is *Davis*.

A year later, working independently, Julia Robinson formulated her hypothesis saying that—roughly speaking—there exists some function

$$\text{“}Exp : \text{” } \mathbf{N} \longrightarrow \mathbf{N}$$

that behaves at least vaguely like an exponential function and whose graph is Diophantine (a *sloppy exponential* would be enough).

Her hypothesis came to be known as “**J.R.**” and explicitly is:

Hypothesis J.R.: There exists a Diophantine set \mathcal{F} of couples (a, b) in $\mathbf{N} \times \mathbf{N}$ with two properties:

- (a) If $(a, b) \in \mathcal{F}$ then $a < b^b$.
- (b) For each positive integer k there is an $(a, b) \in \mathcal{F}$ with $b > a^k$.

Using hypothesis J.R., Robinson shows that the set EXP of triples (a, b, c) with $a = b^c$ is Diophantine, and from this that the set of primes, and the set of factorials is Diophantine as well.

In 1959 Martin Davis and Hillary Putnam showed—assuming that there were arbitrarily long arithmetic progressions of prime numbers—that Hypothesis J.R. implies the equivalence of Diophantine and recursively enumerable, and thereby conditionally establishing a solution to Hilbert’s Tenth Problem (the “conditions” being *the existence of arbitrarily long arithmetic progressions of primes*, and *J.R.*).

A year later, Robinson showed how to avoid the use of the hypothesis that arbitrarily long arithmetic progressions of primes exist, thereby showing that J.R. alone implies a solution to Hilbert’s Tenth Problem (over \mathbf{Z}).

In 1970, Matiyasevich provides a Diophantine definition of a set \mathcal{F} as required by J.R.: he defined his \mathcal{F} to be the collection of pairs (a, b) such that

$$b = F_{2a}$$

where F_n is the n th Fibonacci number, thereby completing the proof that all recursively enumerable sets are Diophantine and establishing the fact that Hilbert's tenth problem (over \mathbf{Z}) is unsolvable.

(I find this quotation of Matiyasevich illuminating:)

“The idea was as follows. A universal computer science tool for representing information uses words rather than numbers. However, there are many ways to represent words by numbers. One such method is naturally related to Diophantine equations. Namely, it is not difficult to show that every 2×2 matrix

$$\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$$

with the m 's being non-negative integers and the determinant $m_{11}m_{22} - m_{12}m_{21}$ equal to 1 can be represented, in a unique way, as a product of matrices

$$M_0 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and

$$M_1 := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

It is evident that any product of such matrices has non-negative integer elements and the determinant equals 1. This implies that we can uniquely represent a word in the two-letter alphabet M_0, M_1 by the four-tuple

$$(m_{11}, m_{12}, m_{21}, m_{22})$$

such that the numbers evidently satisfy the Diophantine equation

$$m_{11}m_{22} - m_{12}m_{21} = 1.$$

Under this representation of words by matrices, the operation of concatenation-of-words corresponds to matrix multiplication and thus can be easily expressed as a system of Diophantine equations, opening up

a way of transforming an arbitrary system of word equations into “equivalent” Diophantine equations. Many decision problems about words had been shown undecidable, so it was quite natural to try to attack Hilbert’s tenth problem by proving the undecidability of systems of word equations.”

...

The focus on cubics!

Here is a list of contexts for which there *are* algorithms to decide whether or not solutions exist over \mathbf{Z} :

- Systems of arbitrarily many polynomials in arbitrary degrees, but in *one* variable
- Systems of arbitrarily many linear polynomials in *many* variables
- A *single* quadratic polynomial in many variables

Here are contexts for which we know there is *no* algorithm to decide whether or not solutions exist over \mathbf{Z} . There is no algorithm that works for every:

- system of arbitrarily many polynomials in many variables of degree ≤ 2
- *single* polynomial of degree 4.

Some of the big unresolved questions for systems of polynomials with coefficients in \mathbf{Z} , then, focus on degree three, and—for example—include:

1. Is there an algorithm to determine whether any given single degree three polynomial in many variables has a solution or not?
2. Is there an algorithm to determine *all* solutions of a single cubic homogenous polynomial in two variables?

I know what I “want the answer to be” (i.e., I want there to be such an algorithm: why not?) but I can’t give any compelling reason for my optimism; nevertheless, our enormous concentrated effort on cubic things (specifically the arithmetic of elliptic curves) seems—so far—to be, at the very least, worth the while.

“Stability” for Elliptic curves and Undecidability over number fields

Thanks to recent work of Shlapentokh and Poonen, one has this amazing further relationship between cubic polynomials in two variables (i.e., elliptic curves) and Hilbert’s Tenth Problem over number fields:

Theorem: Let K be a number field and let \mathcal{O}_K be the ring of integers in K .

If a certain **stability result** in the arithmetic of elliptic curves *that we’ll be discussing in detail in the next hour* holds over K , then every recursively enumerable subset of \mathcal{O}_K is Diophantine in \mathcal{O}_K (in the sense that we have discussed).

The marvelous consequence of this development is that it reduces decidability questions to elliptic curves, one of the most intensely studied facets of arithmetic!

Karl Rubin and I have recently shown that this stability result holds *if you assume the 2-primary part of the classical Shafarevich-Tate Conjecture*.

I'll discuss this at greater length in the subsequent hours, but the important consequence of this conjecture is:

If the Shafarevich-Tate Conjecture is true then the standard known algorithm for finding all rational solutions (over a number field K) of homogenous cubic polynomial equations in two variables (coefficients in K) will terminate finitely.

That is, *if true, we **have** an algorithm to solve these equations of number fields.*

As a consequence, Karl Rubin and I have shown that, conditional on the 2-primary part of the Shafarevich-Tate Conjecture, Hilbert's Tenth problem has a negative answer for the ring of integers in *any* number field.

Note the curious irony in the formulation of our theorem:

If we have a proof of the (2-primary part of the) Shafarevich-Tate conjecture

—*i.e., colloquially speaking: if the algorithm that enables us to deal with arithmetic of cubic plane curves can be **proved** to work—*

then we have a proof of the **non**-existence of a general algorithm for the ring of integers over any number field.

Thanks to a result of Kirsten Eisenträger who has related Hilbert's Tenth Problem over rings of integers in number fields to a much more general class of rings, one gets:

Theorem: Conditional on the 2-primary part of the Shafarevich-Tate Conjecture, Hilbert's Tenth problem has a negative answer for any commutative ring A that is of infinite cardinality, and is finitely generated over \mathbf{Z} .

An Open Question

I have always liked Serge Lang's attitude towards these matters, who—in effect—focussed much attention to the question of determining whether there are finitely many, as opposed to infinitely many, solutions rather than existence or nonexistence of solutions and asked algebro-geometric questions about structure of the infinitely many solutions when they exist.



In this spirit allow me to formulate a question—without prejudice—that seems worth contemplating even if it is a bit premature to try to make much headway with it.

If V is an algebraic variety over \mathbf{Q} let

$$X(V; \mathbf{Q}) \subset V$$

be the Zariski closure in V of the set $V(\mathbf{Q})$ of \mathbf{Q} -rational points of V .

Define $D(V) = D(V; \mathbf{Q}) :=$
the number of irreducible components of $X(V; \mathbf{Q})$.

Suppose that we set out to find upper bounds for this function from algebraic varieties to natural numbers:

$$V \mapsto D(V).$$

Consider, for example, the case where V is an irreducible curve.

- If V is of genus 0, then $D(V)$ is either 0 or 1 depending upon whether V has a rational point or not.
- If V is of genus one, then
 - $D(V)$ is 0 if V has no rational points,
 - $D(V)$ is 1 if V has infinitely many rational points, and
 - $D(V)$ is the order of the Mordell-Weil group of V over \mathbf{Q} , if that group is finite.

In all cases for V of genus one we get that $D(V) \leq 16$.

- If V is of genus > 1 , by Faltings' Theorem $D(V)$ is the (finite) number of rational points of V . Conditional on a conjecture of Lang, Caparoso, Harris and I have shown that $D(V)$ is bounded by a function that depends only on the genus of V .

In sum, we have that (conditional on a conjecture of Lang) for *all algebraic varieties V of dimension one*,

$D(V)$ is bounded from above by a function $F(|V_{\mathbf{C}}|)$ that depends only on the homotopy type $|V_{\mathbf{C}}|$ of the complex analytic space associated to V .

Is the above statement true or false for algebraic surfaces? Or, more generally, for algebraic varieties of arbitrary dimension?

Part II: Elliptic Curves

Recall that in the first lecture we talked of decision procedures for determining whether or not systems of polynomial equations have solutions over the rings of integers of number fields and we were led to

the arithmetic of elliptic curves

and mentioned the relevance of

the Shafarevich-Tate Conjecture.

I will be discussing joint work with Karl Rubin in this theory that relates to Hilbert's Tenth Problem.

A brief introduction to the arithmetic of elliptic curves

Take a typical elliptic curve with rational coefficients such as:

$$\mathcal{E} : Y^2 + XY + Y = X^3 - X^2 -$$

2006776241557552658503320820

9338542750930230312178956502X

+

34481611795030556467032985690390720374855

944359319180361266008296291939448732243429

We call the (smooth) projective curve over \mathbf{Q} cut out by this equation or by any of its more general companions, which in usual notation are written:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with $a_i \in \mathbf{Z}$ and having discriminant nonzero, *elliptic curves*.

They are, in a natural way, algebraic groups: the classical *chord-and-tangent-process* endows the set of (rational) points on such an elliptic curve E (over any number field K) with the structure of an abelian group (called the **Mordell-Weil group** of E over K and denoted $E(K)$).

This group is known to be finitely generated (a theorem almost a century old due to Mordell in the case of $K = \mathbf{Q}$ and generalized by Weil for arbitrary global fields).

So

$$E(K) \approx \mathbf{Z}^r \oplus T(E, K)$$

where:

$r = r(E, K)$ is called the **Mordell-Weil rank of E over K**

and

$T(E, K)$ is the (finite) **torsion subgroup of the Mordell-Weil group.**

In the case of the elliptic curve \mathcal{E} displayed at the beginning of this section, it was shown (by Noam Elkies, 2006) that (it has trivial torsion over \mathbf{Q}) and its Mordell-Weil rank over \mathbf{Q} is at least 28—this being, to my knowledge, the current world’s record for Mordell-Weil ranks over \mathbf{Q} (and if you are curious to see 28 linear independent rational points on this curve, here they are:

Independent points of infinite order:

$$P_1 = [-2124150091254381073292137463, 259854492051899599030515511070780628911531]$$

$$P_2 = [2334509866034701756884754537, 18872004195494469180868316552803627931531]$$

$$P_3 = [-1671736054062369063879038663, 251709377261144287808506947241319126049131]$$

$$P_4 = [2139130260139156666492982137, 36639509171439729202421459692941297527531]$$

$$P_5 = [1534706764467120723885477337, 85429585346017694289021032862781072799531]$$

$$P_6 = [-2731079487875677033341575063, 262521815484332191641284072623902143387531]$$

$$P_7 = [2775726266844571649705458537, 12845755474014060248869487699082640369931]$$

$$P_8 = [1494385729327188957541833817, 88486605527733405986116494514049233411451]$$

$$P_9 = [1868438228620887358509065257, 59237403214437708712725140393059358589131]$$

P10 = [2008945108825743774866542537, 47690677880125552882151750781541424711531]

P11 = [2348360540918025169651632937, 17492930006200557857340332476448804363531]

P12 = [-1472084007090481174470008663, 246643450653503714199947441549759798469131]

P13 = [2924128607708061213363288937, 28350264431488878501488356474767375899531]

P14 = [5374993891066061893293934537, 286188908427263386451175031916479893731531]

P15 = [1709690768233354523334008557, 71898834974686089466159700529215980921631]

P16 = [2450954011353593144072595187, 4445228173532634357049262550610714736531]

P17 = [2969254709273559167464674937, 32766893075366270801333682543160469687531]

P18 = [2711914934941692601332882937, 2068436612778381698650413981506590613531]

P19 = [20078586077996854528778328937, 2779608541137806604656051725624624030091531]

P20 = [2158082450240734774317810697, 34994373401964026809969662241800901254731]

P21 = [2004645458247059022403224937, 48049329780704645522439866999888475467531]

P22 = [2975749450947996264947091337, 33398989826075322320208934410104857869131]

P23 = [-2102490467686285150147347863, 259576391459875789571677393171687203227531]

P24 = [311583179915063034902194537, 168104385229980603540109472915660153473931]

P25 = [2773931008341865231443771817, 12632162834649921002414116273769275813451]

P26 = [2156581188143768409363461387, 35125092964022908897004150516375178087331]

P27 = [3866330499872412508815659137, 121197755655944226293036926715025847322531]

P28 = [2230868289773576023778678737, 28558760030597485663387020600768640028531]

Torsion

The structure of the torsion subgroup part of the Mordell-Weil group is relatively more understood than the rank; for example, any $T(E, K)$ is isomorphic to a subgroup of $\mathbf{Q}/\mathbf{Z} \times \mathbf{Q}/\mathbf{Z}$; and for any given K there are only finitely possible isomorphism types for the $T(E, K)$'s that can occur; and for $K = \mathbf{Q}$ the list of these finitely possible isomorphism types is explicitly known.

Rank

In contrast, very little is known of a general nature regarding the behavior of $r(E, K)$, for varying E and K . I don't know, for example, whether

$$\sup_{E, K} \frac{r(E, K)}{[K : \mathbf{Q}]}$$

is finite when E/K runs over all elliptic curves over all number fields. (I bet no!).

Descent

The standard method—perhaps the only method—of finding upper bounds for $r(E, K)$ for specific elliptic curves E over specific fields K is called

the method of descent

a method that seems to have been already present in some arguments due to Fermat and has been elaborated and refined ever since.

These days “descent” is done via computation of what are called **Selmer groups**. In the third lecture I’ll be a bit more explicit about this method is, but for now, in a few words, here is the “vague shape” of the descent method as it has evolved in present times.

Recall: We are trying to compute the rank of the group $E(K)$ of K -rational points of the elliptic curve E .

First key idea: Note that for any (your choice) integer $N > 1$, if you know the order of the quotient group

$$\frac{E(K)}{N \cdot E(K)}$$

you get an upper bound for $r(E, K)$:

$$r(E, K) \leq \lfloor \log_N \left| \frac{E(K)}{N \cdot E(K)} \right| \rfloor.$$

Second key idea: Construct—for each choice of N —a group whose order is actually

- $\geq |E(K)/NE(K)|$, and
- *computable*,

thereby getting—for each choice of N —a *computable upper bound* for $r(E, K)$.

Third key idea (i.e., hope): that for $N \gg 0$ that upper bound gives $r(E, K)$ exactly!

We do this via *Selmer groups*

Fix the elliptic curve E and the number field K . For each integer $N > 1$ one constructs a certain finite abelian group of exponent N called the *N -Selmer group* $S_N(E, K)$ (this is given by a construction related to Galois cohomology) which has the two key properties required:

- $S_N(E, K)$ is *computable in theory*; i.e., there is indeed a finite algorithm that computes it. Also for $N = 2$ or for certain choice triples (N, E, K) , there is an elaborate technology for actually managing to compute it.
- There is a canonical *injective homomorphism*

$$E(K)/NE(K) \hookrightarrow S_N(E, K)$$

A consequence is that we may obtain—thanks to the above two items—a *computable upper bound for the Mordell-Weil rank* $r(E, K)$.

A computation of the N -Selmer group $S_N(E, K)$ for *any one* $N \geq 2$ provides us with *some* finite upper bound for $r(E, K)$; specifically:

$$r(E, K) \leq \lfloor \log_N |S_N(E, K)| \rfloor.$$

The Shafarevich-Tate Conjecture

Let

$$\mathcal{N} \subset \mathbf{N}$$

be any unbounded set of natural numbers.

By the \mathcal{N} -**Shafarevich-Tate Conjecture**—for (E, K) —we mean the claim that the cardinalities of the *cokernels* of the injective homomorphisms

$$E(K)/NE(K) \hookrightarrow S_N(E, K)$$

admit a (finite) upper bound for all $N \in \mathcal{N}$.

It is evidently equivalent to ask that the numbers

$$\frac{|S_N(E, K)|}{|E(K)/NE(K)|}$$

admit such a finite upper bound.

Or—also equivalently—

$$|S_N(E, K)| = N^{r(E, K)} \times O(1)$$

for all $N \in \mathcal{N}$.

Clearly if for *any single* unbounded set of natural numbers \mathcal{N} the \mathcal{N} -Shafarevich-Tate Conjecture held for (E, K) we would have something better than a mere *upper bound* for the Mordell-Weil rank of E over K !

The conjecture gives us a precise expression for $r(E, K)$, and it would even be nicely computable,

$$r(E, K) = \lim_{N \in \mathcal{N}} \log_N |S_N(E, K)|$$

if one could—in addition—bound the “ $O(1)$ ” occurring in this formula.

By the *Shafarevich-Tate Conjecture for (E, K)* with no prefix we'll mean the \mathbf{N} -Shafarevich-Tate Conjecture. This is indeed eponymously conjectured and this conjecture visibly implies the \mathcal{N} -Shafarevich-Tate Conjecture for any \mathcal{N} .

By the *p -adic Shafarevich-Tate Conjecture* for (E, K) we mean the \mathcal{P} -Shafarevich-Tate Conjecture for (E, K) where \mathcal{P} is the set of all powers of the prime number p .

Although we do have other methods for determining $r(E, K)$ either in special situations or conditional on various standard conjectures—

- via Heegner points and similar constructions,
- order of vanishing of the L -function $L(E, K; s)$ at $s = 1$, or
- (conditional, again) in terms of *mean values of biases*,

Nevertheless *descent via the computation of Selmer groups* stands out as—conjecturally, at least—being the basic perfectly general and reasonably computable method for determining $r(E, K)$.

You

- **by day:** search for rational points, say by increasing heights, and work out their possible dependence relations, getting a monotone increasing sequence of lower bounds for $r(E, K)$ and
- **by night:** compute $\log_N |S_N(E, K)|$ for a chosen succession of increasing values of N getting a monotone decreasing sequence of upper bounds for $r(E, K)$, and
- **hope:** that one day or one night the upper and lower bounds will be equal, giving you a perfectly unconditional computation of $r(E, K)$.

The effect of the Shafarevich-Tate Conjecture (for any single unbounded set \mathcal{N}) is to make the claim that *the above strategy will always succeed* if one lives long enough. It would be very very interesting to quantify how long one has to live to see this algorithm terminate—as an elementary function of the basic numerical data of the input (E, K) .

Back to H10P and Mordell-Weil Stability

The following types of questions, interesting in their own right, seem never to have been focused head-on by number theorists until it was shown that their answers bear interesting consequences for mathematical logic.

Definition Let L/K be an extension (of finite degree) of number fields and let E be an elliptic curve over K . Say that E has **stable Mordell-Weil rank r for L/K** if (it does; i.e., if:)

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

Question

Let L/K be any extension of number fields and $r \geq 0$. Does there exist an elliptic curve E defined over K with stable rank r for L/K ?

Discuss formats of questions in the arithmetic of elliptic curves: applied versus pure issues

It isn't entirely unnatural that such a question might be put to useful purposes in attempting to negotiate between recursively enumerable sets expressed in a Diophantine way over alternatively \mathcal{O}_L and $\mathcal{O}_K \dots$

Discuss

Hilbert's Tenth problem relative to L/K

Let, as above, L/K denote a (finite degree) extension of number fields and $\mathcal{O}_L/\mathcal{O}_K$ the induced extension of rings of integers. It would be pretty elegant if we could just put our finger on a simple finite system of polynomial equations over \mathcal{O}_L that cleanly cut out \mathcal{O}_K as a Diophantine subset of \mathcal{O}_L . The actual constructions, though, are somewhat more complicated, and more sophisticated—beginning with constructions as in the work of Matiyasevich, continued by Denef, Denef-Lipschitz, Pheidas, and more recently Poonen and Shlapentokh:

Theorem (Poonen, Shlapentokh): Assume there exists an elliptic curve E defined over K with stable rank $r > 0$ for L/K . Then if every recursively enumerable subset of \mathcal{O}_K is Diophantine, then every recursively enumerable subset of \mathcal{O}_L is Diophantine.

Karl Rubin and I are thankful to Bjorn Poonen for mentioning to us the following easy corollary of this theorem:

Corollary: If for every Galois (cyclic) extension of number fields L/K of prime degree there exists an L/K -stable elliptic curve, then for any number field K any recursively enumerable subset of \mathcal{O}_K is Diophantine over \mathcal{O}_K .

It would follow, then, from the hypothesis of this corollary that Hilbert's Tenth Problem would have a negative solution for the ring of integers in any number field.

Karl Rubin and I assume (at least a part of) the 2-adic Shafarevich-Tate Conjecture and we prove:

Theorem: Assume the 2-adic Shafarevich-Tate Conjecture. Then for every prime degree Galois extension L/K of number fields there is an L/K -stable elliptic curve of rank $r = 1$.

Hence—again “modulo 2-adic Shafarevich-Tate”—we establish the negative result for Hilbert’s Tenth Problem over the ring of integers of an arbitrary number field.

Collections of field extensions

Let K be a field and \bar{K}/K an algebraic closure of K . By a *small subextension* of \bar{K}/K let us mean a field extension M/L where $K \subset L \subset M \subset \bar{K}$ and such that $[M : K]$ is finite.

Let \mathcal{D} be a collection of small subextensions of \bar{K}/K . Suppose that \mathcal{D} is closed under these three operations.

1. *intersection* : if $M/L_1, M/L_2$ are in \mathcal{D} then $M/L_1 \cap L_2$ is in \mathcal{D} .
2. *smaller sub-extensions with the same base*:
If $L \subset N \subset M$ and M/L is in \mathcal{D} then so is N/L .
3. *composition*: If M/N and N/L are in \mathcal{D} , so is M/L .

Lemma: If \mathcal{D} is a collection of small subextensions of \bar{K}/K closed under the above three operations, then \mathcal{D} consists of *all* small subextensions if and only if \mathcal{D} contains all small subextensions M/L that are cyclic of prime degree.

Proof. Note first that if \mathcal{D} contains all small subextensions M/L that are cyclic of prime degree—i.e., if \mathcal{D} satisfies the hypotheses of our lemma—and if \mathcal{D} is closed under composition (item (3)) above) then \mathcal{D} contains all cyclic extensions. Assume this.

Now let M/L be an arbitrary *Galois* small subextension. Since \mathcal{D} contains all cyclic small subextensions, for every element

$$\sigma \in G := \text{Gal}(M/L)$$

we have that M/M^σ is in \mathcal{D} , (here M^σ is the fixed subfield of σ). Since $L = \bigcap_{\sigma \in G} M^\sigma$ and since \mathcal{D} is closed under intersection (item (1)) above) we have that M/L is in \mathcal{D} .

It then follows that for any small subextension M/L its Galois closure over L is in \mathcal{D} . Consequently since \mathcal{D} is closed under smaller subextensions with the same base (item (2)) above) M/L is also in \mathcal{D} .

Diophantine subsets in rings of algebraic integers

Put $K = \mathbf{Q}$. From now on, by *small subextension* with no further qualifier we mean small subextension of $\bar{\mathbf{Q}}/\mathbf{Q}$. For L/K let \mathcal{O}_L denote the ring of integers in L . Say that a small subextension M/L is **integrally Diophantine** if \mathcal{O}_L is Diophantine in \mathcal{O}_M . Let \mathcal{D} be the collection of *integrally Diophantine* small subextensions.

Proposition: The collection \mathcal{D} of integrally Diophantine small subextensions is closed under the operations (1), (2), (3) listed above.

Proof. Closure under the operation (1) follows since an intersection of Diophantine sets is Diophantine. As for closure under (2) and (3) the argument is (awkward to write out, but) an exercise.

In order to prove our theorem, Rubin and I were led to develop sharp methods to control 2-Selmer rank, and these methods have some side consequences that answer—also raise—some natural questions.

Here are examples of two such results that we prove unconditionally:

Theorem 0.1 *Given any number field K there is an elliptic curve E over K such that there are many quadratic characters χ of K such that the twisted elliptic curve E^χ has no non-trivial rational points over K .*

Note: We can even take E to be the base change to K of an elliptic curve over \mathbf{Q} .

Theorem 0.2 *If K is not totally imaginary, and E is any elliptic curve over K with no nontrivial K -rational 2-torsion, there are many quadratic characters χ of K such that the twisted elliptic curve E^χ has no nontrivial rational points over K .*

Notes:

- By *many quadratic characters* we only mean to say that the number of characters χ with $N_{K/\mathbf{Q}} \text{cond}_K(\chi) < X$ that gives the conclusion of the theorem is $\gg X/\log^a(X)$ for some positive number¹ a .
- Over the field $K = \mathbf{Q}$ Ono-Skinner have proven (using Kolyvagin et al) a similar result to Theorem ?? by showing the analogous statement for central values of L functions.
- The lower bound “ $\gg X/\log^a(X)$ ” is unfortunately weak: it is expected that the set of χ 's satisfying the conclusion of Theorem ?? is of positive density, and—in fact—of density $1/2$.

¹This number $a = 2/3$ or $a = 1/3$ according as the action of the Galois group on $E[2]$ is $\text{GL}_2(\mathbf{F}_2)$ or cyclic of order three.

As hinted above, our method is to study the 2-Selmer group of an elliptic curve, and more specifically to see how tightly we can control changes in the rank (i.e., dimension over \mathbf{F}_2) of the 2-Selmer group as one twists the original elliptic curve by quadratic characters. So, in the next lecture I'll discuss Selmer groups in slightly more technical detail.

But allow me to end with two questions we still don't know the answer to:

Given any elliptic curve E over a number field K and any finite extension L/K . Is there a quadratic twist of E that has Mordell-Weil stability for L/K and Mordell-Weil rank ≤ 1 ?

Which hyperelliptic curves over a number field K have the property that for any finite extension L/K they possess quadratic twists C over K that

$$C(L) = C(K) \neq \emptyset?$$