Hilbert's Tenth Problem

Brandon Fodden

University of Lethbridge

January 30, 2012

Note: Much of this talk is based on the Martin Davis paper *Hilbert's Tenth Problem is Unsolvable* (see references)

The problem

Given in Hilbert's 1900 address before the International Congress of Mathematicians.

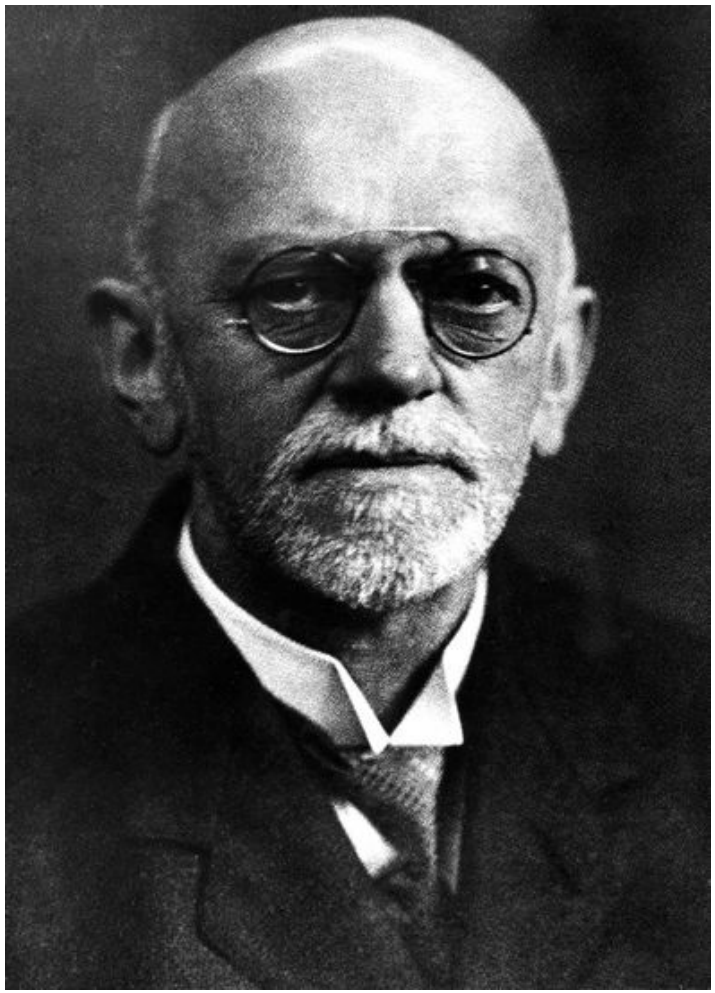
Entscheidung der Lösbarkeit einer diophantischen Gleichung. Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoeffizienten sei vorgelegt: man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

In English:

Given a Diophantine equation with any number of unknown quantities and with integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in integers.

Our goal is to show that no such process (algorithm) may exist!

David Hilbert



We will consider the problem of whether or not a Diophantine equation with integer coefficients has a solution in the *positive integers*.

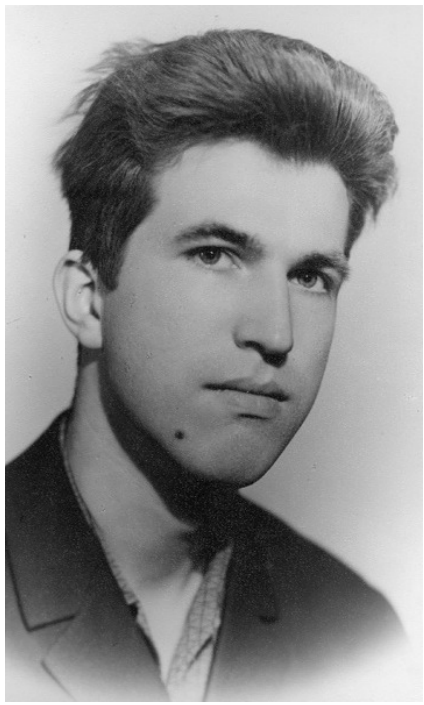
Suppose had an algorithm for testing for solutions in the positive integers. If we want to use it test a Diophantine equation for solutions in the integers, just replace each integer variable x with $x_1 - x_2$ where x_1 and x_2 are positive integer variables.

Now suppose had an algorithm for testing for solutions in the integers. If we want to use it test a Diophantine equation for solutions in the positive integers, just replace each positive integer variable x with $x_1^2 + x_2^2 + x_3^2 + x_4^2 + 1$ where x_1, x_2, x_3 and x_4 are integer variables. This works since every positive integer is the sum of four squares (Lagrange).

Key Players

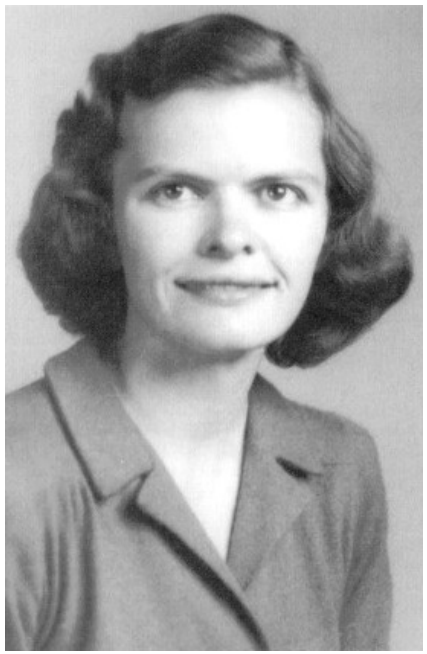
Martin Davis

Yuri Matiyasevich



Hilary Putnam

Julia Robinson



In what follows, all work is due to some subset of these four people, unless otherwise noted.

Diophantine sets

Instead of starting with a Diophantine equation and looking for its solutions, we will begin with a set of 'solutions' and seek a corresponding Diophantine equation.

Definition: A set S of ordered n-tuples of positive integers is called *Diophantine* if there is a polynomial $P(x_1, ..., x_n, y_1, ..., y_m)$ with integral coefficients such that

$$(x_1, ..., x_n) \in S \leftrightarrow (\exists y_1, ..., y_m)(P(x_1, ..., x_n, y_1, ..., y_m) = 0).$$

Here $y_1, ..., y_m$ are positive integers. For now on, all variables represent positive integers unless otherwise stated.

Diophantine sets

Examples of Diophantine sets:

The composite numbers:

$$x \in S \leftrightarrow (\exists y, z)(x = (y+1)(z+1)).$$

Numbers which are not powers of 2:

$$x \in S \leftrightarrow (\exists y, z)(x = y(2z+1)).$$

The set S of (x, y, z) for which $x \mid y$ and $x < z$:

We have $x \mid y \leftrightarrow (\exists u)(y = ux)$ and $x < z \leftrightarrow (\exists v)(z = x + v)$, so

$$(x, y, z) \in S \leftrightarrow (\exists u, v)((y - ux)^2 + (z - x - v)^2 = 0)$$

What about the prime numbers? What about powers of 2?

Diophantine sets

We may use a simultaneous system $P_1 = 0, P_2 = 0, ..., P_k = 0$ of polynomial equations to define a Diophantine set, since the system can be replaced by the equation $P_1^2 + P_2^2 + ... + P_k^2 = 0$.

Theorem (Putnam): A set S of positive integers is Diophantine if and only if there is a polynomial P such that S is equal to the set of positive integers in the range of P.

Proof: (reverse direction): We have

$$x \in S \leftrightarrow (\exists y_1, ..., y_m)(x = P(y_1, ..., y_m)),$$

so S is Diophantine.

(forward direction): S is Diophantine, so there is a polynomial Q such that

$$x \in S \leftrightarrow (\exists y_1, ..., y_m)(Q(x, y_1, ..., y_m) = 0).$$

Let $P(x, y_1, ..., y_m) = x(1 - Q^2(x, y_1, ..., y_m))$. We must show the positive range of P is equal to S.

Let $x \in S$ and choose $y_1, ..., y_m$ so that $Q(x, y_1, ..., y_m) = 0$. Then $P(x, y_1, ..., y_m) = x$, so x is in the positive range of P.

Now let $z > 0$ be in the range of P. Then

$$z = P(x, y_1, ..., y_m) = x(1 - Q^2(x, y_1, ..., y_m))$$

for some $x, y_1, ..., y_m$. Since $z > 0$, we must have $Q(x, y_1, ..., y_m) = 0$. Thus $z = x$ and $x \in S$.

Thus S is the positive range of $P(x, y_1, ..., y_m) = x(1 - Q^2(x, y_1, ..., y_m))$.

Positive range

Using our previous examples, we have

The set of composite numbers is equal to the positive range of

$$x\left(1-[x-(y+1)(z+1)]^2\right)$$

$$=2x^2-2xy-2xz-x^3-xy^2-xz^2+2x^2yz+2x^2y+2x^2z$$

$$-xy^2z^2-2xy^2z-2xyz^2-4xyz.$$

The set of numbers which are not powers of 2 is equal to the positive range of

$$x\left(1-[x-y(2z+1)]^2\right).$$

Diophantine functions

Definition: A (positive integer valued) function of n (positive integer) arguments is called *Diophantine* if

$$\{(x_1, ..., x_n, y) : y = f(x_1, ..., x_2)\} \text{ is a Diophantine set.}$$

We will require a few important Diophantine functions.

Theorem: Let $P(x, y)$ be the Diophantine function $\frac{(x+y-2)(x+y-1)}{2} + y$. $P(x, y)$ is a bijection between the ordered pairs of positive integers and the positive integers. There are Diophantine functions $L(z)$ and $R(z)$ such that

- $\forall x, y, \quad L(P(x, y)) = x$ and $R(P(x, y)) = y$.
- $\forall z$, $P(L(z), R(z)) = z$ (that is, the ordered pair which is mapped to z by $P(x, y)$ is $(L(z), R(z))$).
- $L(z) \leq z$, $R(z) \leq z$.

Diophantine functions

Theorem: (Sequence Number Theorem) There is a Diophantine function $S(i, u)$ such that

- $S(i, u) \leq u$
- For each sequence $a_1, ..., a_N$, there is a number u such that $S(i, u) = a_i$ for $1 \leq i \leq N$.

All finite sequences are 'encoded' in $S(i, u)$. The proof uses the Chinese Remainder Theorem.

The exponential function

By the late 1960s, only one piece was missing in order to show that the algorithm Hilbert asked for can not exist:

$$\text{The exponential function } h(n,k) = n^k \text{ is Diophantine.}$$

Many people thought this was unlikely.

In 1970, Matiyasevich showed the exponential function is Diophantine by using the Fibonacci numbers:

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2}.$$

The key property he used is that

$$F_n^2 \mid F_m \rightarrow F_n \mid m.$$

The Pell equation

Julia Robinson later replaced the Fibonacci numbers with the non-negative solutions to the Pell equation

$$x^2 - dy^2 = 1 \text{ where } d = a^2 - 1 \text{ for } a > 1.$$

Let

$$x_0 = 1, \quad x_1 = a, \quad x_n = 2ax_{n-1} - x_{n-2}$$

and

$$y_0 = 0, \quad y_1 = 1, \quad y_n = 2ay_{n-1} - y_{n-2}.$$

One may show that the non-negative solutions to the Pell equation are the pairs (x_n, y_n).The key property needed is that

$$y_n^2 \mid y_m \rightarrow y_n \mid m.$$

The exponential function is Diophantine

One may show that $m = n^k$ if and only if the following equations have a solution in the remaining arguments:

- $x^2 - (a^2 - 1)y^2 = 1$
- $u^2 - 16(a^2 - 1)r^2y^4 = 1$
- $(x + cu)^2 - ((a + u^2(u^2 - a))^2 - 1)(k + 4(d - 1)y)^2 = 1$
- $y = k + e - 1$
- $(x - y(a - n) - m)^2 = (f - 1)^2(2an - n^2 - 1)^2$
- $m + g = 2an - n^2 - 1$
- $w = n + h = k + \ell$
- $a^2 - (w^2 - 1)(w - 1)^2z^2 = 1$

The factorial is Diophantine

One may show the following theorem: For any positive integer k, if $(2k)^k \leq n$ and $n^k < p$ then

$$k! < \frac{(n+1)^k p^k}{\text{rem}((p+1)^n, p^{k+1})} < k! + 1,$$

where $\text{rem}(x, y)$ is the remainder when y is divided by x.

Using this, one may give a Diophantine definition of the factorial function.

Wilson's Theorem: $k+1$ is prime if and only if $k! \equiv -1 \pmod{k+1}$.

Using Wilson's Theorem, one may now give a Diophantine definition of the set of prime numbers!

Using this Diophantine definition of the primes together with Putnam's Theorem, the following prime representing polynomial was given by Jones, Sato, Wada and Wiens.

A prime representing polynomial

The set of prime numbers is equal to the positive range of

$$
\begin{aligned}
(k+2)\Big[& 1-[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2 \\
& -[2n+p+q+z-e]^2-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2 \\
& -[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2 \\
& -[16r^2y^4(a^2-1)+1-u^2]^2-[n+\ell+v-y]^2 \\
& -[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2 \\
& -[(a^2-1)\ell^2+1-m^2]^2-[ai+k+1-\ell-i]^2 \\
& -[p+\ell(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2 \\
& -[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2 \\
& -[z+p\ell(a-p)+t(2ap-p^2-1)-pm]^2\Big]
\end{aligned}
$$

Note: As it is written here, the variables are non-negative integers.

More prime representing polynomials

Similar polynomials have been written out for the set of Mersenne primes, the set of Fermat primes and the set of 'younger' twin primes.

Positive range polynomials have been written down for the set of even perfect numbers, the set of all perfect numbers, the set of Lucas numbers, and the set of Fibonacci numbers.

(Jones) The set of Fibonacci numbers is equal to the positive range of

$$2y^4x + y^3x^2 - 2y^2x^3 - y^5 - yx^4 + 2y.$$

Back to showing the algorithm Hilbert asked for does not exist...

Universal quantification

An important result is that one may universally quantify over one of the variables in a Diophantine set to obtain another Diophantine set, as long as the quantification is *bounded*.

That is, if P is a polynomial, then

$$S = \{(y, x_1, ..., x_n) : (\forall z)_{\leq y}(\exists y_1, ..., y_m)[P(y, z, x_1, ..., x_n, y_1, ..., y_m) = 0]\}$$

is Diophantine. One must show that

$$(\forall z)_{\leq y}(\exists y_1, ..., y_m)[P(y, z, x_1, ..., x_n, y_1, ..., y_m) = 0]$$

$$\leftrightarrow$$

A large number of expressions, all of which are known to be Diophantine.

I'm not kidding when I say that it won't fit on one slide.

Recursive functions

Another Diophantine definition of the prime numbers:

x is prime $\leftrightarrow (x > 1) \wedge (\forall y, z)_{\leq x}[(yz < x) \vee (yz > x) \vee (y = 1) \vee (z = 1)]$

Actually, our available methods to show a set is Diophantine are quite powerful.

Definition: The recursive (or computable) functions are those that may be computed by a finite program or computing machine having arbitrarily large amounts of time and memory at its disposal (*ie* a Turing Machine).

One may properly define the recursive functions using a small number of initial functions and several recursive operations (composition, primitive recursion, minimalization).

Theorem: A function is Diophantine if and only if it is recursive.

An enumeration of the Diophantine sets

The following construction is based on the aforementioned paper by Davis.

Any polynomial with positive integer coefficients can be constructed from 1 and variables $x_0, x_1, ...$ by successive additions and multiplications. Let

- $P_1 = 1$
- $P_{3i-1} = x_{i-1}$
- $P_{3i} = P_{L(i)} + P_{R(i)}$
- $P_{3i+1} = P_{L(i)} \cdot P_{R(i)}$

Let

$$D_n = \{x_0 : (\exists x_1, ..., x_n)[P_{L(n)}(x_0, x_1, ..., x_n) = P_{R(n)}(x_0, x_1, ..., x_n)]\}$$

Clearly

$$D_1, D_2, D_3, ...$$

consists of all Diophantine sets of positive integers.

A universal Diophantine set

Universality Theoerm:

$$\{(n, x) : x \in D_n\} \text{ is Diophantine.}$$

To prove this, one may show that $x \in D_n$ if and only if there exists u such that the following hold:

- $S(1, u) = 1$
- $S(2, u) = x$
- $(\forall i)_{\leq n}[S(3i, u) = S(L(i), u) + S(R(i), u)]$
- $(\forall i)_{\leq n}[S(3i + 1, u) = S(L(i), u) \cdot S(R(i), u)]$
- $S(L(n), u) = S(R(n), u)$.

Clearly each of these is Diophantine.

Jones has written down a polynomial for the Diophantine definition of $\{(n, x) : x \in D_n\}$.

A non-Diophantine set

Using the enumeration of the Diophantine sets, one may employ a standard diagonalization technique to construct a set that is different from each Diophantine set:

Theorem: $V = \{n : n \notin D_n\}$ is not Diophantine.

Proof: Suppose V were Diophantine. Then $V = D_i$ for some particular i. Is $i \in V$? We have $i \in V \leftrightarrow i \in D_i$ and $i \in V \leftrightarrow i \notin D_i$. This is a contradiction.

A non-recursive function

Theorem: The function

$$g(n,x) = \begin{cases} 1 & \text{if } x \notin D_n \\ 2 & \text{if } x \in D_n \end{cases}$$

is not recursive.

Proof: If g were recursive, then it would be Diophantine, so

$$y = g(n,x) \leftrightarrow (\exists y_1, ..., y_m)[P(n,x,y,y_1,...,y_m) = 0].$$

V is the set of x such that $g(x,x) = 1$, so

$$V = \{x : (\exists y_1, ..., y_m)[P(x,x,1,y_1,...,y_m) = 0]\}.$$

That is, V is Diophantine, which is a contradiction.

Main Theorem

The Universality Theorem yields

$$x \in D_n \leftrightarrow (\exists y_1, ..., y_m)[P(n, x, y_1, ..., y_m) = 0]$$

for some polynomial P (which has been written down by Jones).

Suppose we had an algorithm which determines whether or not a Diophantine equation has positive integer solutions.

For a given n, x, we could use this algorithm to test whether or not $P(n, x, y_1, ..., y_m) = 0$ has a solution.

That is, we could use the algorithm to test whether or not $x \in D_n$.

Thus we could use the algorithm to compute $g(n, x)$, and so $g(n, x)$ must be recursive.

This is a contradiction! No such algorithm may exist!!

Thus Hilbert's Tenth Problem is unsolvable!!!

Diophantine sets

We can also give a nice description of the Diophantine sets.

Definition: A set S of n-tuples of positive integers is recursively enumerable (or listable) if there are recursive functions $f(x, x_1, ..., x_n)$ and $g(x, x_1, ..., x_n)$ such that

$$S = \{(x_1, ..., x_n) : (\exists x)[f(x, x_1, ..., x_n) = g(x, x_1, ..., x_n)]\}.$$

It is not hard to show that a set is Diophantine if and only if it is recursively enumerable.

Diophantine sets are the listable sets.

An application

Let $P(n)$ be a decidable property of the positive integers (that is, we have an algorithm which will determine whether or not P holds for any given n). Let $S = \{n : P(n) \text{ is false}\}$. Since P is decidable, S is recursively enumerable (listable).

Thus S is Diophantine. We have

$$P(n) \text{ is false} \leftrightarrow n \in S \leftrightarrow (\exists y_1, ..., y_m)[Q(n, y_1, ..., y_m) = 0],$$

and so

$$\begin{aligned} \forall n P(n) &\leftrightarrow \forall n \neg(\exists y_1, ..., y_m)[Q(n, y_1, ..., y_m) = 0] \\ &\leftrightarrow \neg(\exists n, y_1, ..., y_m)[Q(n, y_1, ..., y_m) = 0]. \end{aligned}$$

Thus we have

$$\forall n P(n) \leftrightarrow Q \text{ has no solutions in the positive integers.}$$

An application

Goldbach's conjecture:

$$\forall n[n \text{ even} \rightarrow (\exists_{\leq n} p)(p \text{ is prime and } n - p \text{ is prime})].$$

Thus there is a particular Diophantine equation which has no solutions if and only if Goldbach's conjecture is true.

Let $\delta(x) = \prod_{n<x} \prod_{p^k \leq n} p$ where p represents a prime. The Riemann Hypothesis is equivalent to

$$\forall n \left[\left(\sum_{k \leq \delta(n)} \frac{1}{k} - \frac{n^2}{2} \right)^2 < 36n^3 \right]$$

Thus there is a particular Diophantine equation which has no solutions if and only if the Riemann Hypothesis is true.

Determining if a Diophantine equation has solutions is a *very* hard problem! Also: imagine what could be done if Hilbert's algorithm existed!

A formal application

The set of theorems of a formal axiomatic system (such as ZFC set theory or Peano arithmetic) is recursively enumerable.

Let $P(n)$ be "there is no contradiction among the first n theorems."

This is a decidable property.

Thus there is a particular Diophantine equation which has no solutions if and only if the formal system is consistent.

Gödel's second incompleteness theorem implies that no formal system which allows basic arithmetic may prove its own consistency.

Thus the formal system is not strong enough to prove that the Diophantine equation has no solutions.

Open problems

Hilbert's Tenth Problem for a ring R: Given a Diophantine equation with integral numerical coefficients: Can one find an algorithm which determines whether the equation has solutions in R?

- $R = \mathbb{Z}$: No (we just saw this)
- $R = \mathbb{C}$: Yes
- $R = \mathbb{R}$: Yes
- $R = \mathbb{Q}$: open (note: an algorithm for $\mathbb{Z}$ would have given one for $\mathbb{Q}$.)
- $R = \mathcal{O}_K$: Conjecture is no. Known for totally real K, quadratic extensions of totally real K, and K which have one conjugate pair of non-real embeddings.

Theorem (Poonen, Shlapentokh) If there is an elliptic curve $E/\mathbb{Q}$ with

$$\text{rank}E(K) = \text{rank}E(\mathbb{Q}) = 1,$$

then Hibert's Tenth Problem for $\mathcal{O}_K$ is a negative answer.

Further information

- M. Davis, *Hilbert's Tenth Problem is unsolvable,* American Mathematical Monthly, vol. 80 (1973), pages 233-269.
- M. Davis, Y. Matiyasevich and J. Robinson, *Hilbert's Tenth Problem: positive aspects of a negative solution,* Proceedings of the Symposium on the Hilbert Problems, AMS, 1976, pages 323-378.
- J.P. Jones, D. Sato, H. Wada and D. Wiens, *Diophantine representation of the set of prime numbers,* American Mathematical Monthly, vol. 83 (1976), pages 449-464.
- Y. Matiyasevich, *Hilbert's Tenth Problem*, MIT Press (1993).
- M. Davis, *Hilbert's Tenth Problem* video lecture, Convergence of Logic, Math. and Comp. Sci., UCLA. Available on iTunes U.