Hilbert's Tenth Problem

Anna Gow

Carleton University

July 2017

David Hilbert

The Problem

- In Hilbert's native tongue, German:

  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.

The Problem

- In Hilbert's address before the International Congress of Mathematicians, he stated that "…every definite mathematical problem must necessarily be susceptible of a precise settlement, either in the form of an actual answer to the question asked, or *by the proof of the impossibility of its solution…*".

- The combined works of Martin Davis, Yuri Matiyasevich, Hilary Putnam, and Julia Robinson proved that the answer to Hilbert's Tenth Problem is that *no such algorithm can exist*.

Davis, Matiyasevich, Putnam, Robinson

The Problem

- Note that showing that we can test a Diophantine equation for solutions in the integers is equivalent to showing that we can test for solutions in the positive integers.
- Suppose there exists an algorithm which could test any particular Diophantine equation for positive integral solutions. To test for solutions in the integers, we can simply replace each integer variable x with $x_1 - x_2$, where x_1 and x_2 are positive integers.
- Conversely, suppose there exists an algorithm for testing integral solutions. To test for solutions in the positives, we can replace each positive integer variable x with $x_1^2 + x_2^2 + x_3^2 + x_4^2 + 1$, where $x_1,\ldots, x_4$ are integers (by Lagrange's four-square theorem).

Diophantine Sets

- **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.
- From now on, all variables will represent positive integers, unless otherwise specified.
- Which sets are Diophantine?

Diophantine Sets

- The numbers which are not powers of 2:

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

- The composite numbers:

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

- The divisibility relation - that is, $S = \{(x,y) : x \mid y\}$:

  $$(x,y) \in S \leftrightarrow (\exists u)[y = ux]$$

- The ordering relation – that is, $S = \{(x,z) : x < z\}$:

  $$(x,z) \in S \leftrightarrow (\exists v)[z = x + v]$$

Diophantine Sets

- The set S such that $x \mid y$ and $x < z$:

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

- The set S such that $x \mid y$ or $x < z$:

$$(x,y,z) \in S \leftrightarrow (\exists u,v)[(y-ux)(z-x-v) = 0]$$

Diophantine Sets

- **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:**

In the reverse direction, it is easy to see that if S is related to $P(x_1, ..., x_m)$ as stated then:

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

Conversely, let:

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

Diophantine Sets

- **Proof:**

Let $P(x, y_1, \ldots, y_m) = x[1 - Q^2(x, y_1, \ldots, y_m)]$. We want to show that the positive range of P is equal to S.

For $x \in S$, take $y_1, \ldots, y_m$ such that $Q(x, y_1, \ldots, y_m) = 0$.

In this case, $P(x, y_1, \ldots, y_m) = x$ (so x is in the range of P).

Now let $z \geq 1$ be in the range of P. So:

$$z = P(x, y_1, \ldots, y_m) = x[1 - Q^2(x, y_1, \ldots, y_m)]$$

Here, we must have $Q(x, y_1, \ldots, y_m) = 0$.

Thus $z = x$ and $x \in S$.

So S is the positive range of $P(x, y_1, \ldots, y_m) = x[1 - Q^2(x, y_1, \ldots, y_m)]$.

Diophantine Functions

- **Definition:** A function of n arguments is called Diophantine if:

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

- Which functions are Diophantine?

Diophantine Functions

- The exponential function:

$$f(n,k) = n^k$$

- The binomial function:

$$g(n,k) = \binom{n}{k}$$

- The factorial function:

$$h(n) = n!$$

Recursive Functions/Sets

- **Definition 1:** A function is said to be recursive (computable) if it may be computed by a finite program or computing machine with arbitrarily large amounts of time and memory at its disposal (a Turing Machine).

- **Definition 2:** A set S of positive integers is called recursive (decidable) if there exists a recursive function f such that:

  $f(n) = 1$ for all $n \in S$,

  $f(n) = 0$ for each $n \notin S$

Recursively Enumerable Sets

- **Definition:** A set S of positive integers is said to be recursively enumerable (listable) if it is the range of some recursive function f.

Important Theorems

- **Theorem 1:** There exists a set S of positive integers that is recursively enumerable but is not recursive.
- For such a set, there exists an algorithm that lists all the elements in S, but an algorithm which tells you if some arbitrary positive integer is in S cannot exist.
- **Theorem 2 (DMPR):** A function is Diophantine if and only if it is recursive.
- **Theorem 3 (DMPR):** A set is Diophantine if and only if it is recursively enumerable.

Prime Representing Polynomial

- The previous theorems allow us to deduce that the set of prime numbers is Diophantine (since we can list them).
- Using Putnam's theorem (proved earlier in slides) we can construct a prime generating polynomial.
- Jones, Sata, Wada, and Wiens wrote down one such polynomial (of degree 25 in 26 variables):

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

The Proof

- Let S be a set of positive integers that is recursively enumerable but not recursive.
- Since S is recursively enumerable, it is Diophantine.
- Thus, there exists some polynomial P where $x \in S$ exactly when there exist some positive integers $y_1, ..., y_m$ with $P(x, y_1, ..., y_m) = 0$.
- Suppose there is a positive solution to Hilbert's Tenth Problem. That is, there exists an algorithm to determine whether or not a Diophantine equation has solutions.

The Proof

- For any given x, we could use such an algorithm on our polynomial P to determine whether or not there exist positive integers $y_1, \ldots, y_m$ such that $P(x, y_1, \ldots, y_m) = 0$.
- That is, the algorithm determines whether or not $x \in S$.
- Thus S is recursive, a contradiction.

An Application

- Let $P(n)$ be a decidable property of the positive integers. That is, there exists an algorithm which correctly determines whether or not P holds for any given positive integer n.
- We can show that $S = \{n : P(n) \text{ is false}\}$ is a Diophantine set.
- That is:

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

- So we have:

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

- Thus:

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

An Application

- **Goldbach's conjecture:** Every even integer greater than 2 can be written as the sum of two primes.
- Goldbach's conjecture is decidable.
- Thus, there is a particular Diophantine equation which has no solutions if and only if Goldbach's conjecture is true.

An Application

- **The Riemann Hypothesis:** The Riemann zeta function has zeroes only at the even negative integers and at complex numbers in the form $\frac{1}{2} + bi$, where b is a real number.
- One of the most important open problems in Number Theory!
- The Riemann Hypothesis is decidable (and its equivalent Diophantine equation is still in progress).

Further Reading

- M. Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly 80 (1973), 233-269.

Fin