Unsolvability of Hilbert's Tenth Problem

Jun Le Goh

University of Wisconsin-Madison

Logic Assoc. of Malaysia Introductory Logic Course
February 2022

Hilbert's tenth problem

Hilbert ($\approx$ 1900, translated to English by Newson):

> *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 by a finite number of operations whether the equation is solvable in rational integers.*

What is a "process [which uses] a finite number of operations"?

This was defined in the 1940s by work of Gödel, Herbrand, Church, Post and Turing.

In 1970, Matiyasevich (building on work of Davis, Putnam and Robinson) showed that there cannot be such a process.

References

My primary references for these lectures are:

1. Davis, *Hilbert's tenth problem is unsolvable*
   American Mathematical Monthly, vol. 80, 1973
2. Jones and Matiyasevich, *Proof of recursive unsolvability of Hilbert's tenth problem*
   American Mathematical Monthly, vol. 98, 1991

Diophantine equations

$$x + 2y - 3 = 0$$

$$x^2 + y^2 - z^2 = 0$$

$$x^3 + y^3 - z^3 = 0$$

$$x^2 - 2y^2 - 1 = 0$$

$$y^2 - x^3 + 36x = 0$$

Hilbert's tenth problem asks for a process to determine whether equations such as the above have any integer solutions.

Examples of equations which we know how to solve

Proposition

The linear equation $ax + by = c$ has an integer solution (x, y) if and only if

$$\gcd(a, b) \text{ divides } c.$$

Proposition

The quadratic equation $x^2 + y^2 = 3z^2$ has no integer solutions (x, y, z).

Proof.

Suppose (x, y, z) is an integer solution. WLOG $\gcd(x, y) = 1$.

If 3 divides x, then $x^2 \equiv 0 \pmod 3$, else $x^2 \equiv 1 \pmod 3$. Same for y.

Since 3 cannot divide both x and y, we have

$$x^2 + y^2 \equiv 1 \text{ or } 2 \pmod 3.$$

This contradicts $3z^2 \equiv 0 \pmod 3$. □

Changing the scope from $\mathbb{Z}$ to $\mathbb{N}$

Proposition

$P(x_1, \ldots, x_n) = 0$ has a solution in $\mathbb{Z}$ if and only if $P(a_1 - b_1, \ldots, a_n - b_n) = 0$ has a solution in $\mathbb{N}$.

Theorem

$P(x_1, \ldots, x_n) = 0$ has a solution in $\mathbb{N}$ if and only if

$$P(p_1^2 + q_1^2 + r_1^2 + s_1^2, \ldots, p_n^2 + q_n^2 + r_n^2 + s_n^2) = 0$$

has a solution in $\mathbb{Z}$.

To prove ($\Rightarrow$) of the theorem, use a theorem of Lagrange:

> *Every natural number can be expressed as the sum of squares of four (possibly zero) integers, i.e., for every $c \in \mathbb{N}$, $p^2 + q^2 + r^2 + s^2 = c$ has some solution $(p, q, r, s) \in \mathbb{N}^4$.*

Diophantine relations

Definition

A relation $S \subseteq \mathbb{N}^n$ is a Diophantine relation if there is some Diophantine equation $P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$ such that

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

(The scope of $y_1, \ldots, y_m$ is $\mathbb{N}$.)

- x is *not* a power of 2 if and only if

$$(\exists y, z)[x - y(2z + 3) = 0].$$

- x is *not* prime if and only if

$$(\exists y, z)[x - (y + 2)(z + 2) = 0].$$

Diophantine relations

Definition (repeated)

A relation $S \subseteq \mathbb{N}^n$ is a Diophantine relation if there is some Diophantine equation $P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$ such that

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

- x divides y if and only if
$$(\exists d)[y - dx = 0].$$
- $x < z$ if and only if
$$(\exists v)[x + v + 1 - z = 0].$$
- x is the remainder of y when divided by z if and only if $\exists q(y = qz + x)$ and $x < z$ if and only if
$$(\exists d, v)[(y - dz - x)^2 + (x + v + 1 - z)^2 = 0].$$

Closure properties of Diophantine relations

Lemma

Diophantine relations are closed under intersection and union.

Proof.

Suppose S_1 and S_2 are Diophantine relations which are defined by

$$\exists \overline{y} P_1(\overline{x}, \overline{y}) = 0 \qquad \text{and} \qquad \exists \overline{z} P_2(\overline{x}, \overline{z}) = 0$$

respectively. Then $S_1 \cap S_2$ is defined by

$$\exists \overline{y}, \overline{z}[P_1(\overline{x}, \overline{y})^2 + P_2(\overline{x}, \overline{z})^2 = 0].$$

$S_1 \cup S_2$ is defined by

$$\exists \overline{y}, \overline{z}[P_1(\overline{x}, \overline{y}) \cdot P_2(\overline{x}, \overline{z}) = 0].$$

□

Closure properties of Diophantine relations

A Diophantine function is one whose graph is a Diophantine relation.

Lemma

Diophantine functions are closed under composition.

Proof.

Suppose f is an m-ary Diophantine function and $g_1, \ldots, g_m$ are Diophantine functions. Then

$$z = f(g_1(\overline{x_1}), \ldots, g_m(\overline{x_m}))$$

if and only if

$$\exists y_1, \ldots, y_m (z = f(y_1, \ldots, y_m) \wedge y_1 = g_1(\overline{x_1}) \wedge \cdots \wedge y_m = g_m(\overline{x_m})).$$

By substituting the Diophantine definitions of $f, g_1, \ldots, g_m$ into the above, we may obtain a Diophantine definition of the composition. □

Section 1

Diophantine $\Leftrightarrow$ recursive

Diophantine $\Leftrightarrow$ recursive

Our goal in this section is to prove

Theorem

The Diophantine functions are exactly the recursive functions.

Proposition

Every Diophantine function is recursive.

Sketch.

Suppose f is a Diophantine function which is defined by

$$z = f(\overline{x}) \quad \Leftrightarrow \quad \exists \overline{y} P(\overline{x}, z, \overline{y}) = 0.$$

Given natural numbers $\overline{x}, z, \overline{y}$, one can compute whether $P(\overline{x}, z, \overline{y}) = 0$. We know that for each $\overline{x}$, there is exactly one z for which there are $\overline{y}$ with $P(\overline{x}, z, \overline{y}) = 0$. Therefore we can recursively find such z by minimization. $\square$

Towards recursive $\Rightarrow$ Diophantine: Primitive recursion

Recall that the recursive functions are closed under primitive recursion.

So we need to show that the Diophantine functions are closed under primitive recursion, i.e.,

> *If f and g are n-ary and $(n+2)$-ary Diophantine functions respectively, then the following $(n+1)$-ary function h is Diophantine:*
>
> $$h(\overline{x}, 0) = f(\overline{x})$$
> $$h(\overline{x}, t+1) = g(\overline{x}, t, h(\overline{x}, t)).$$

Towards recursive $\Rightarrow$ Diophantine: Encoding sequences

Goal: Show that if f and g are n-ary and $(n+2)$-ary Diophantine functions respectively, then the following $(n+1)$-ary function h is Diophantine:

$$h(\overline{x}, 0) = f(\overline{x})$$
$$h(\overline{x}, t+1) = g(\overline{x}, t, h(\overline{x}, t)).$$

One needs to construct a Diophantine equation which defines the "history" of the computation which produces $h(\overline{x}, t)$, i.e.,

$$h(\overline{x}, 0), h(\overline{x}, 1), \ldots, h(\overline{x}, t-1), h(\overline{x}, t).$$

For fixed t, one can easily do this. For example, for $t = 2$,

$$y = h(\overline{x}, 2) \quad \Leftrightarrow \quad (\exists y_0, y_1)(y_0 = f(\overline{x}) \wedge y_1 = g(\overline{x}, 0, y_0) \wedge y = g(\overline{x}, 1, y_1)).$$

But we need a single Diophantine definition which works for all t, so we need to encode each "history" as a *single* number, rather than using a new existential quantifier for each entry in the "history".

Towards encoding sequences: Encoding pairs

Theorem (Pairing)

There are Diophantine functions $P(x, y)$, $L(z)$ and $R(z)$ such that

1. *for all x, y, $L(P(x, y)) = x$ and $R(P(x, y)) = y$;*
2. *for all z, $P(L(z), R(z)) = z$;*
3. *for all z, $L(z), R(z) \leq z$.*

Proof.

Consider the Cantor pairing function $(x, y) \mapsto \frac{(x+y)(x+y+1)}{2} + y$. Formally,

$$\begin{aligned} z = P(x, y) \quad &\text{if} \quad 2z = (x + y)(x + y + 1) + 2y \\ x = L(z) \quad &\text{if} \quad \exists y[2z = (x + y)(x + y + 1) + 2y] \\ x = R(z) \quad &\text{if} \quad \exists x[2z = (x + y)(x + y + 1) + 2y]. \end{aligned}$$

It follows from invertibility of the Cantor pairing function that $L(z)$ and $R(z)$ are functions. □

Encoding sequences using sequence numbers

Theorem (Sequence numbers)

There is a Diophantine function $S(i, u)$ such that $S(i, u) \leq u$ and for each sequence $a_1, \ldots, a_n$, there is some u such that $S(i, u) = a_i$ for each i.

(Think of u as a code for the sequence $a_1, \ldots, a_n$. Think of $S(i, u)$ as extracting the ith entry of the sequence encoded by u.)

Proof.

Define $S(i, u)$ to be the remainder of $L(u)$ divided by $1 + i \cdot R(u)$.

Since L, R, and remainder are Diophantine functions and Diophantine functions are closed under composition, $S(i, u)$ is Diophantine.

Also, $S(i, u) \leq L(u) \leq u$.

To show that each sequence $a_1, \ldots, a_n$ is encoded by some u, we use the Chinese remainder theorem (next slide).

Encoding sequences using sequence numbers, continued

Theorem (Sequence numbers)

There is a Diophantine function $S(i, u)$ such that $S(i, u) \leq u$ and for each sequence $a_1, \ldots, a_n$, there is some u such that $S(i, u) = a_i$ for each i.

Proof. (continued)

($S(i, u)$ is the remainder of $L(u)$ divided by $1 + i \cdot R(u)$.)

Given $a_1, \ldots, a_n$, we can construct u as follows. Fix any $y > a_1, \ldots, a_n$ which is divisible by $n!$. Then

$$1 + y, \quad 1 + 2y, \quad \ldots, \quad 1 + ny$$

are relatively prime. The Chinese remainder theorem gives us x s.t.

$$x \equiv a_i \pmod{1 + iy} \qquad \text{for } i = 1, \ldots, n.$$

Then we could take $u = P(x, y)$. □

Towards recursive $\Rightarrow$ Diophantine: Bounded quantification

Theorem

If $P(b, z, \overline{x}, \overline{y}) = 0$ is Diophantine, then the set of $(b, \overline{x})$ s.t.

$$(\forall z \leq b)(\exists \overline{y})[P(b, z, \overline{x}, \overline{y}) = 0]$$

is Diophantine.

In other words, the class of Diophantine relations is closed under bounded quantification.

The proof of this theorem is very long. Before we dive in, we shall derive some corollaries.

The set of prime numbers is Diophantine

Recall that the set of composite numbers is easily seen to be Diophantine:

$$x \text{ is composite} \quad \Leftrightarrow \quad (\exists y, z)[x - (y+2)(z+2) = 0].$$

Theorem
The set of prime numbers is Diophantine.

Proof.
x is prime if and only if

$$x > 1 \wedge (\forall y, z \leq x)(yz < x \vee yz > x \vee y = 1 \vee z = 1).$$

By the theorem on bounded quantification, the above yields a Diophantine definition. □

Corollaries of closure under bounded quantification

Corollary

The Diophantine functions are closed under primitive recursion.

Proof.

Suppose f and g are n-ary and $(n+2)$-ary Diophantine functions respectively. Let h denote the $(n+1)$-ary function defined by primitive recursion:

$$h(\overline{x}, 0) = f(\overline{x})$$
$$h(\overline{x}, t+1) = g(t, h(\overline{x}, t), \overline{x}).$$

Observe that $y = h(\overline{x}, z)$ if and only if there are u, v such that:

1. $v = S(0, u)$ and $v = f(\overline{x})$
2. for all $t < z$, there is some w such that $w = S(t+1, u)$ and $w = g(t, S(t, u), \overline{x})$
3. $y = S(z, u)$.

This shows that h is Diophantine; note the bounded universal quantifier over t. □

Corollaries of closure under bounded quantification

Corollary

The Diophantine functions are closed under minimization.

Proof.

Suppose f is an $(n+1)$-ary Diophantine function such that for each n-tuple $\overline{x}$, there is some y such that $f(\overline{x}, y) = 0$.

For each $\overline{x}$, define $h(\overline{x})$ to be the least y such that $f(\overline{x}, y) = 0$.

We have $y = h(\overline{x})$ if and only if $f(\overline{x}, y) = 0$ and for all $t < y$, $f(\overline{x}, t) > 0$.

This shows that h is Diophantine; note the bounded universal quantifier over t. □

What's next

Combining the corollaries on the previous two slides, one can prove

Theorem

Every recursive function is Diophantine.

Returning now to bounded quantification, a major intermediate step is to prove

Theorem (Matiyasevich 1970)

The exponential function $(n, k) \mapsto n^k$ *is Diophantine.*

Matiyasevich's theorem provided the final piece needed to show that Hilbert's tenth problem is unsolvable:

Theorem (Davis, Putnam, Robinson 1961)

Hilbert's tenth problem for exponential Diophantine equations is unsolvable.

Exponential is Diophantine: Pell's equation $x^2 - dy^2 = 1$

If (x, y) is a solution with $y \neq 0$, then $\frac{x}{y} \approx \sqrt{d}$. It is closely connected to the continued fraction expansion of $\sqrt{d}$.

Historical notes:

- Important contributions were made by Greek and Indian mathematicians such as Brahmagupta (7th century AD).
- It appears that Brouncker (≈ 1650) was the first to give a method for finding all solutions, while Lagrange (≈ 1750) was the first to give a method with what we might consider a proof.
- It seems that Pell had a very small role, if any: Dickson blames Euler for this misattribution (see chapter XII in Dickson, *History of the theory of numbers*, vol. II, 1966)

Exponential is Diophantine: Pell's equation $x^2 - dy^2 = 1$

We will focus on the case $d = a^2 - 1$ for integers $a \geq 2$.

Theorem

$(x, y) \in \mathbb{N}^2$ is a solution to $x^2 - (a^2 - 1)y^2 = 1$ if and only if there is some $k \geq 0$ such that

$$(a + \sqrt{a^2 - 1})^k = x + y\sqrt{a^2 - 1}.$$

Definition

For each $k \in \mathbb{N}$, define $x_k(a)$ and $y_k(a)$ by

$$(a + \sqrt{a^2 - 1})^k = x_k(a) + y_k(a)\sqrt{a^2 - 1}.$$

Exponential is Diophantine: Pell's equation $x^2 - (a^2 - 1)y^2 = 1$

Definition (repeated)

Define $x_k(a)$ and $y_k(a)$ by $(a + \sqrt{a^2 - 1})^k = x_k(a) + y_k(a)\sqrt{a^2 - 1}$.

k	$x_k(a)$	$y_k(a)$
0	1	0
1	a	1
2	$2a^2 - 1$	$2a$
3	$4a^3 - 3a$	$4a^2 - 1$

The polynomials $x_k(a)$ and $y_k(a)$ are known as Chebyshev polynomials. They are closely related to trigonometric addition formulas, e.g.,

$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta) \qquad \text{and} \qquad \frac{\sin(3\theta)}{\sin(\theta)} = 4\cos^2(\theta) - 1.$$

Recurrences for x_k and y_k

The plan now is to use $(x_k(a))_k$ and $(y_k(a))_k$ to define the exponential function.

Lemma

$$x_{k+1} = a \cdot x_k + (a^2 - 1) \cdot y_k \qquad x_{k+1} = 2a \cdot x_k - x_{k-1}$$
$$y_{k+1} = a \cdot y_k + x_k \qquad y_{k+1} = 2a \cdot y_k - y_{k-1}$$

Now we can reason about $(x_k(a))_k$ and $(y_k(a))_k$ using induction on k.

For example, one can prove by induction on k that

Lemma

$(x_k(a))_k$ grows exponentially, specifically, for each k we have $a^k \leq x_k(a) \leq (2a)^k$.

Robinson's congruence

Lemma (Robinson 1952)

n^k and $x_k - (a-n)y_k$ are equal modulo $2an - n^2 - 1$.

Proof.

Induction on k. For the inductive step, modulo $2an - n^2 - 1$, we have

$$
\begin{aligned}
& x_{k+1} - (a-n)y_{k+1} \\
&= (2ax_k - x_{k-1}) - (a-n)(2ay_k - y_{k-1}) && \text{recurrences} \\
&= 2a(x_k - (a-n)y_k) - (x_{k-1} - (a-n)y_{k-1}) \\
&\equiv 2an^k - n^{k-1} && \text{ind. hyp.} \\
&= n^{k-1}(2an - 1) \\
&\equiv n^{k-1}(n^2) \\
&= n^{k+1}.
\end{aligned}
$$

□

Corollary of Robinson's congruence

Corollary

Suppose $n \geq 2$ and $k \geq 1$. For every $a > x_k(n)$, n^k is the remainder of $x_k(a) - (a-n)y_k(a)$ divided by $2an - n^2 - 1$.

Proof.

By Robinson's congruence, it suffices to show that $n^k < 2an - n^2 - 1$. We have

$$\begin{aligned} n^k &\leq x_k(n) && \text{by growth rate of } (x_k(n))_k \\ &< a && \text{by assumption} \\ &\leq 2an - n^2 - 1, \end{aligned}$$

where the last inequality holds because

$$\begin{aligned} a(2n-1) &\geq (n+1)(2n-1) && a > n^k \geq n \\ &> n^2 + 1 && n \geq 2. \end{aligned}$$

Towards showing that $x_k(a)$ and $y_k(a)$ are Diophantine

The corollary to Robinson's congruence shows that the exponential function is Diophantine, assuming that $x_k(a)$ and $y_k(a)$ are Diophantine.

To prove the latter, we need more properties about $x_k(a)$ and $y_k(a)$.

First, we have lemmas which relate $y_k(a)$ and a (roughly).

Lemma (Robinson 1952)
$a - 1$ *divides* $y_k(a) - k$.

Closely related is

Lemma
$a - b$ *divides* $y_k(a) - y_k(b)$.

First and Second Step Down Lemmas

Next, we have lemmas which relate $y_q(a)$ and q (roughly).

Lemma (SDL1)

$y_k(a)^2$ divides $y_q(a)$ if and only if $k \cdot y_k(a)$ divides q.

Lemma (SDL2)

$y_r(a) \equiv \pm y_p(a) \pmod{x_q(a)}$ if and only if $r \equiv \pm p \pmod{2q}$.

Diophantine definition of $x_k(a)$ and $y_k(a)$

Theorem

(a, k, c, d) satisfies $c = x_k(a)$ and $d = y_k(a)$ if and only if there are $e, f, g, h, i \in \mathbb{N}$ such that:

1. $c^2 - (a^2 - 1)d^2 = 1$
2. $e^2 - (a^2 - 1)f^2 = 1$
3. $h^2 - (g^2 - 1)i^2 = 1$
4. $2d^2$ *divides* f
5. $g \equiv a \pmod{e}$
6. $g \equiv 1 \pmod{2d}$
7. $i \equiv k \pmod{2d}$
8. $i \equiv d \pmod{e}$
9. $k \leq d$.

Diophantine definition of $x_k(a)$ and $y_k(a)$, forward direction

Suppose $c = x_k(a)$ and $d = y_k(a)$. Define

$$\begin{array}{lll} q = k \cdot y_k(a) & e = x_{2q}(a) & f = y_{2q}(a) \\ g = a + e^2(e^2 - a) & h = x_k(g) & i = y_k(g) \end{array}$$

4. $2d^2$ divides f: By SDL1, since $k \cdot y_k(a)$ divides q, we have $y_k(a)^2$ $(= d^2)$ divides $y_q(a)$. Now $f = y_{2q}(a) = 2x_q(a)y_q(a)$ (by a "double angle formula"), so $2d^2$ divides f.
5. $g \equiv a \pmod{e}$ by definition of g.
6. $g \equiv 1 \pmod{2d}$: By (2), $e^2 \equiv 1 \pmod{f^2}$. It follows from (4) that $e^2 \equiv 1 \pmod{2d}$. So $g \equiv 1 \pmod{2d}$, by definition of g.
7. $i \equiv k \pmod{2d}$: By (6), $2d$ divides $g - 1$. By Robinson, $g - 1$ divides $y_k(g) - k$ $(= i - k)$. So $i \equiv k \pmod{2d}$.
8. $i \equiv d \pmod{e}$: By (5), e divides $g - a$. Also, $g - a$ divides $y_k(g) - y_k(a)$ $(= i - d)$. So $i \equiv d \pmod{e}$.

Backward direction

Suppose there are e, f, g, h, i such that:

1. $c^2 - (a^2 - 1)d^2 = 1$
2. $e^2 - (a^2 - 1)f^2 = 1$
3. $h^2 - (g^2 - 1)i^2 = 1$
4. $2d^2$ divides f
5. $g \equiv a \pmod{e}$
6. $g \equiv 1 \pmod{2d}$
7. $i \equiv k \pmod{2d}$
8. $i \equiv d \pmod{e}$
9. $k \leq d$.

By 1–3, let p, q, r be such that $c = x_p(a)$, $d = y_p(a)$, $e = x_q(a)$, $f = y_q(a)$, $h = x_r(g)$, $i = y_r(g)$.

Claim: $k = p$ (so $c = x_k(a)$ and $d = y_k(a)$).

Notice $p \leq y_p(a) = d$ and $k \leq d$. So it suffices to show

$$k \equiv \pm p \pmod{2d}.$$

By (7) we have $k \equiv i \pmod{2d}$. We also have

$$i \equiv r \pmod{2d}$$

by (6) and Robinson:

$$2d \quad \text{divides} \quad g - 1 \quad \text{divides} \quad y_r(g) - r = i - r.$$

It remains to show $r \equiv \pm p \pmod{2d}$.

Backward direction, cont.

Suppose there are e, f, g, h, i such that:

1. $c^2 - (a^2 - 1)d^2 = 1$
2. $e^2 - (a^2 - 1)f^2 = 1$
3. $h^2 - (g^2 - 1)i^2 = 1$
4. $2d^2$ divides f
5. $g \equiv a \pmod{e}$
6. $g \equiv 1 \pmod{2d}$
7. $i \equiv k \pmod{2d}$
8. $i \equiv d \pmod{e}$
9. $k \leq d$.

Let p, q, r be such that $c = x_p(a)$, $d = y_p(a)$, $e = x_q(a)$, $f = y_q(a)$, $h = x_r(g)$, $i = y_r(g)$.

Goal: $r \equiv \pm p \pmod{2d}$.

First, we show that d divides q:

$$(4) \quad \Rightarrow \quad y_p(a)^2 \mid y_q(a) \quad \overset{\text{SDL1}}{\Rightarrow} \quad y_p(a) \mid q.$$

Therefore it suffices to show $r \equiv \pm p \pmod{2q}$.

By (8),

$$y_r(g) \equiv y_p(a) \pmod{x_q(a)}.$$

By (5) and a previous lemma,

$$x_q(a) = e \quad \text{divides} \quad g - a \quad \text{divides} \quad y_r(g) - y_r(a),$$

so

$$y_r(a) \equiv y_p(a) \pmod{x_q(a)}.$$

By SDL2, $r \equiv \pm p \pmod{2q}$. □

Recap

We showed that $(a, k) \mapsto x_k(a)$ and $(a, k) \mapsto y_k(a)$ are Diophantine.

This implies (by Robinson's congruence) that $(n, k) \mapsto n^k$ is Diophantine.

Our next goal is to show that the class of Diophantine relations is closed under bounded quantification.

To do this, we shall show that several other functions are Diophantine.

More Diophantine functions

Theorem

The following functions are Diophantine:

$$(n, k) \mapsto \binom{n}{k}$$

$$n \mapsto n!$$

$$(a, t, y) \mapsto \prod_{k \leq y} (a + kt)$$

We shall briefly discuss the ideas involved in proving the above.

Binomial coefficient is Diophantine

Main idea: $\binom{n}{k}$ is the kth digit in the base u expansion of $(u+1)^n$, whenever u is large enough.

Lemma

If $k \leq n$ and $u > 2^n$, then $\binom{n}{k}$ is the remainder of $\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor$ when divided by u.

Proof.

First, $\binom{n}{k} < 2^n < u$. Second, by the binomial theorem,

$$\frac{(u+1)^n}{u^k} = \underbrace{\sum_{i=0}^{k-1} \binom{n}{i} u^{i-k}}_{\text{less than 1}} + \binom{n}{k} + \underbrace{\sum_{i=k+1}^{n} \binom{n}{i} u^{i-k}}_{\text{divisible by } u}.$$

□

Factorial and "Product" are Diophantine

Lemma

For each k, we have

$$k! = \left\lfloor (2k)^{k^2} / \binom{(2k)^k}{k} \right\rfloor.$$

Using the above lemma, we can show that $n \mapsto n!$ is Diophantine.

Lemma

Fix a, t and y. If q and u satisfy $qt \equiv a \pmod{u}$ and $u > \prod_{k \leq y}(a + kt)$, then $\prod_{k \leq y}(a + kt)$ is the remainder of

$$\prod_{k \leq y}(qt + kt) \qquad \left(= t^{y+1}(y+1)! \binom{q+y}{y+1} \right)$$

when divided by u.

Using the above lemma, we can show that $(a, t, y) \mapsto \prod_{k \leq y}(a + kt)$ is Diophantine.

Bounded quantification is Diophantine

Theorem (repeated from many slides ago)

If $P(k, b, \overline{x}, \overline{y}) = 0$ *is Diophantine, then the set of* $(b, \overline{x})$ *s.t.*

$$(\forall k \leq b)(\exists \overline{y})[P(k, b, \overline{x}, \overline{y}) = 0]$$

is Diophantine.

Some observations which play a key role in the proof: Let p be a prime.

1. If p divides $P(y)$ and $p > |P(y)|$, then $P(y) = 0$.
2. If $y' \equiv y \pmod{p}$, then $P(y') \equiv P(y) \pmod{p}$.
3. If c and q are such that p divides $1 + c \cdot q!$, then $p > q$.

Bounded quantification is Diophantine

Sketch of proof of theorem on previous slide.

Using P, define a polynomial $Q(b, u, x)$ such that:

- $Q(b, u, x) > \max\{b, u\}$
- $Q(b, u, x) > |P(k, b, x, y)|$ whenever $k \leq b$ and $y \leq u$.

One can show that $(\forall k \leq b)(\exists y)(P(k, b, x, y) = 0)$ if and only if there are u, k', t, y' such that:

- $t = Q(b, u, x)!$
- $1 + k't = \prod_{k \leq b}(1 + kt)$
- $1 + k't$ divides $\prod_{y \leq u}(y' - y)$
- $1 + k't$ divides $P(k', b, x, y')$.

□

Together with previous results, this completes the proof that a function is Diophantine if and only if it is recursive.

Diophantine sets = recursively enumerable sets

Theorem

The Diophantine sets are exactly the recursively enumerable sets.

Proof.

Suppose $S = \{x \in \mathbb{N} : \exists \overline{y} P(x, \overline{y}) = 0\}$ is a Diophantine set. Then S is the projection of the recursive set $\{(x, \overline{y}) : P(x, \overline{y}) = 0\}$, so S is r.e.

Conversely, suppose $S \subseteq \mathbb{N}$ is r.e. Then S is the range of a recursive function $f : \mathbb{N} \to \mathbb{N}$. We have proved that recursive functions are Diophantine, so we can write

$$z = f(x) \quad \Leftrightarrow \quad \exists \overline{y} P(z, x, \overline{y}) = 0.$$

Then $z \in S$ if and only if $\exists x, \overline{y} P(z, x, \overline{y}) = 0$. □

Section 2

Applications to Hilbert's tenth problem

Proof that Hilbert's tenth problem is unsolvable

Theorem

There is a Diophantine equation $P(x, \overline{y}) = 0$ for which there is no recursive function $f : \mathbb{N} \to \{0, 1\}$ such that $f(x) = 1 \Leftrightarrow \exists \overline{y} P(x, \overline{y}) = 0$.

So there is a family of Diophantine equations $(P(x, \overline{y}) = 0)_{x \in \mathbb{N}}$ for which Hilbert's tenth problem is already unsolvable.

Proof.

Fix an r.e. set S which is not recursive (e.g., the halting problem.) Since S is r.e., it is Diophantine. Fix $P(x, \overline{y})$ such that

$$S = \{x \in \mathbb{N} : \exists \overline{y} P(x, \overline{y}) = 0\}.$$

Since S is not recursive, there cannot be any recursive function f such that $f(x) = 1 \Leftrightarrow \exists \overline{y} P(x, \overline{y}) = 0$. □

How unsolvable is Hilbert's tenth problem?

We have just showed that Hilbert's tenth problem is unsolvable, but how unsolvable is it? Recursion theory allows us to quantify this.

Fix an effective encoding of each Diophantine equation as a natural number.

Then we can view Hilbert's tenth problem as a subset of $\mathbb{N}$:

$$\mathrm{HTP} := \{e \in \mathbb{N} : e \text{ is a code for a Diophantine equation which has a solution}\}.$$

We shall prove

Theorem

HTP *is Turing equivalent to the halting problem* K*, i.e.,* HTP *is computable with oracle* K *and vice versa. In fact, they are equivalent under many-one reducibility.*

K is at least as complicated as HTP

Proposition

HTP *is many-one reducible to* K*, i.e., there is a recursive function* f *such that for each* e*,* $f(e)$ *lies in* K *if and only if the Diophantine equation coded by* e *has a solution.*

The point here is that HTP is r.e., and every r.e. set is many-one reducible to K. We sketch a direct proof here:

Sketch.

Consider the following machine M:

> *Given input* (e, n)*,* M *begins by ignoring* n *and decoding* e *to obtain a Diophantine equation* $P(\overline{x}) = 0$*. Then* M *tries all tuples* $\overline{x}$ *one by one, to see if* $P(\overline{x}) = 0$*. If it finds some such* $\overline{x}$*, then it halts.*

By the Church-Turing thesis, M is implemented by a partial recursive function $g(e, n)$. Define a recursive function $f : \mathbb{N} \to \mathbb{N}$ as follows: $f(e)$ is an index for the partial recursive function $n \mapsto g(e, n)$. □

HTP is as complicated as K

Theorem

Every r.e. set S is many-one reducible to HTP, i.e., for each r.e. set S, there is a recursive function $f : \mathbb{N} \to \mathbb{N}$ such that for each x, the number x lies in S if and only if the Diophantine equation coded by $f(x)$ has a solution.

In particular, K is many-one reducible to HTP.

Proof.

Since S is r.e., it is Diophantine. Fix $P(x, \overline{y})$ such that

$$S = \{x \in \mathbb{N} : \exists \overline{y} P(x, \overline{y}) = 0\}.$$

For each x, define $f(x)$ to be the code of the Diophantine equation $P(x, \overline{y}) = 0$. □

Therefore HTP is exactly as complicated as K (as measured by relative computability as well as many-one reducibility).

Post's problem on r.e. sets

Quoting from Post (1944) (reformatted):

> *For unsolvable problems the concept of reducibility leads to the concept of degree of unsolvability:*
>
> - *two unsolvable problems being of the same degree of unsolvability if each is reducible to the other,*
> - *one of lower degree of unsolvability than another if it is reducible to the other, but that other is not reducible to it,*
> - *of incomparable degrees of unsolvability if neither is reducible to the other.*
>
> *[..] (Among the r.e. unsolvable problems) there is certainly a highest degree of unsolvability. Our whole development largely centers on the single question of whether there is, among these problems, a lower degree of unsolvability than that, or whether they are all of the same degree of unsolvability.*

Section 3

Subproblems and variations of Hilbert's tenth problem

Subproblems which are known to be solvable or unsolvable

Question

Which subproblems of Hilbert's tenth problem are solvable?

Degree one: Exercise for you.

One variable: Exercise for you.

Degree two, two variables: Solved by Lagrange (≈ 1800).

Degree two, arbitrarily many variables: Solved by Siegel (1972).

Degree three remains open. In the two variable case, much is known.

Degree three, two variables

Theorem (Baker 1970s)

All integer solutions (x, y) *to*

$$y^2 = ax^3 + bx^2 + cx + d$$

satisfy

$$|x|, |y| < \exp((10^6 \cdot \max(|a|, |b|, |c|, |d|))^{10^6}).$$

Corollary

There is an algorithm to decide whether a given equation of the form $y^2 = ax^3 + bx^2 + cx + d$ *has any integer solution.*

Proof.

Check every x and y with $|x|, |y| < \exp((10^6 \max(|a|, |b|, |c|, |d|))^{10^6})$. □

Degree four

Proposition

Given any Diophantine equation $P(x_1, \ldots, x_n) = 0$, we can compute a Diophantine equation $Q(y_1, \ldots, y_m) = 0$ of degree 4, which has an integer solution if and only if the original equation has an integer solution.

Proof.

We shall construct a system of Diophantine equations of degree 2. Then we can consider the sum of their squares to obtain a single equation of degree 4.

To do so, perform the following substitution repeatedly: Replace a term of degree $d > 2$ with a term of degree 2 using a new variable. For example, we can replace x^4 with xy and add a new equation $y = x^3$. Then we would replace x^3 with xz and add a new equation $z = x^2$. □

Corollary

Hilbert's tenth problem for Diophantine equations of degree at most 4 is unsolvable.

Notice the above procedure comes at the cost of increasing the number of variables.

Number of variables

The best result I know is:

Theorem (Sun 1992)

Hilbert's tenth problem for Diophantine equations with at most 11 variables is unsolvable.

Computational complexity of subproblems of Hilbert's tenth problem

Computational complexity is concerned with the time and/or space resources needed to solve computational problems.

The computational complexity of number-theoretic problems, such as factoring, is central to the analysis of cryptographic schemes such as RSA.

Whenever a subproblem of Hilbert's tenth problem is solvable, we can ask: What is its computational complexity?

Computational complexity of subproblems of Hilbert's tenth problem

Theorem (Baker 1970s, repeated from before)

All integer solutions (x, y) *to*

$$y^2 = ax^3 + bx^2 + cx + d$$

satisfy

$$|x|, |y| < \exp((10^6 H)^{10^6}),$$

where $H = \max(|a|, |b|, |c|, |d|)$.

The naive algorithm arising from Baker's theorem has "high" time complexity: One tests each of the x and y with $|x|, |y| < \exp((10^6 H)^{10^6})$.

For certain other classes of equations, one can do better: See Lagarias (2011) and its references.

Generalizations of subproblems of Hilbert's tenth problem

Consider the following problem for fixed k:

Given a Diophantine equation of degree $\leq k$, decide if it has solutions in $\mathbb{N}$.

It is easy to reduce Hilbert's tenth problem for equations for degree $\leq k$ to the above problem.

The converse is not clear, however.

Even though deciding whether a given Diophantine equation has solutions in $\mathbb{N}$ can be reduced to Hilbert's tenth problem, this reduction does not preserve degree.

Example

$x_1^2 + 3x_2 + 2 = 0$ has a solution in $\mathbb{N}$ if and only if

$$(p_1^2 + q_1^2 + r_1^2 + s_1^2)^2 + 3(p_2^2 + q_2^2 + r_2^2 + s_2^2) + 2 = 0$$

has a solution in $\mathbb{Z}$.

Generalizations of subproblems of Hilbert's tenth problem

Theorem (Grunewald, Segal 2004)

There is an algorithm which takes in a Diophantine equation of degree 2 and decides whether it has solutions in $\mathbb{N}$. In fact, there is an algorithm which can decide whether the equation has finitely or infinitely many solutions in $\mathbb{N}$.

Notice that in general, the set of Diophantine equations with infinitely many solutions in $\mathbb{N}$ (or in $\mathbb{Z}$) is not (obviously) recursively enumerable.

Nevertheless we can still express such a property using a first-order sentence.

Deciding truth of first-order sentences

For each statement

$$P(x_1, \ldots, x_n) = 0 \text{ has a solution in } \mathbb{Z},$$

there is a first-order sentence φ in the language $+, \cdot, 0, 1, =$:

$$(\exists x_1)(\exists x_2) \ldots (\exists x_n) P(x_1, \ldots, x_n) = 0$$

such that the statement holds if and only if φ is true in the structure $(\mathbb{Z}, +, \cdot, 0, 1)$.

Definition

The *first-order theory* of a structure is the set of first-order sentences which are true in said structure.

Deciding truth of first-order sentences in $\mathbb{Z}$

Just as we defined codes for Diophantine equations, we can define codes for all first-order sentences. Therefore we can think of the first-order theory of a structure as a subset of $\mathbb{N}$.

General question: For each structure, is its first-order theory recursive?

Theorem
The first-order theory of $(\mathbb{Z}, +, \cdot, 0, 1)$ *is not recursive.*

Sketch.
Hilbert's tenth problem is unsolvable. □

Deciding truth of first-order sentences in $\mathbb{C}$

Theorem ("essentially" "classical")

The first-order theory of $(\mathbb{C}, +, \cdot, 0, 1)$ *is recursive.*

This holds because there is an effective procedure for converting a first-order formula φ to a quantifier-free formula which is equivalent to φ in the structure $(\mathbb{C}, +, \cdot, 0, 1)$.

We call this effective quantifier elimination.

Corollary

Hilbert's tenth problem for $\mathbb{C}$ *is solvable.*

Deciding truth of first-order sentences in $\mathbb{R}$

$(\mathbb{R}, +, \cdot, 0, 1)$ does not admit quantifier elimination:

$$\exists y(x = y^2)$$

is not equivalent to a quantifier-free formula in the language $+, \cdot, 0, 1$.

Theorem (Tarski 1951)

The expanded structure $(\mathbb{R}, +, \cdot, 0, 1, \leq)$ *admits effective quantifier elimination. So its first-order theory is recursive.*

Corollary

The first-order theory of $(\mathbb{R}, +, \cdot, 0, 1)$ *is recursive. Hilbert's tenth problem for* $\mathbb{R}$ *is solvable.*

Hilbert's tenth problem for rings other than $\mathbb{Z}$

There are several rings of interest to number theorists other than $\mathbb{Z}$.

We just discussed $\mathbb{C}$ and $\mathbb{R}$. What about $\mathbb{Q}$?

For $\mathbb{Q}$ and subfields K of $\overline{\mathbb{Q}}$, Hilbert's tenth problem is open, i.e., it is not known if there is an algorithm which decides whether a given Diophantine equation has solutions in $\mathbb{Q}$ (K respectively).

Hilbert's tenth problem for $\mathbb{Q}$

Proposition

Suppose $\mathbb{Z}$ is existentially definable over $\mathbb{Q}$. Then Hilbert's tenth problem for $\mathbb{Q}$ is unsolvable.

Sketch.

$P(x_1, \ldots, x_n) = 0$ has a solution in $\mathbb{Z}$ if and only if

$$\exists x_1, \ldots, x_n \in \mathbb{Q}(P(\overline{x}) = 0 \wedge x_1 \in \mathbb{Z} \wedge \cdots \wedge x_n \in \mathbb{Z}).$$

If "$x_i \in \mathbb{Z}$" is existential, then the above can be reformulated as "$Q(\overline{y}) = 0$ has a solution in $\mathbb{Q}$" for some Diophantine $Q(\overline{y})$. The desired result follows from unsolvability of Hilbert's tenth problem for $\mathbb{Z}$. □

It is not known if $\mathbb{Z}$ is existentially definable over $\mathbb{Q}$. But it is possible to define $\mathbb{Z}$ in $\mathbb{Q}$ using a first-order formula in the language $+, \cdot, 0, 1, =$.

Defining $\mathbb{Z}$ in $\mathbb{Q}$ using a first-order formula

- In 1949, Robinson was the first to define $\mathbb{Z}$ in $\mathbb{Q}$ using a first-order formula. Her formula had the form $\forall\exists\forall$.
- In 2009, Poonen found a formula of the form $\forall\exists$.

Building on Poonen's work, Koenigsmann showed:

Theorem (Koenigsmann 2016)

There is a polynomial $P(x, y_1, \ldots, y_n)$ with coefficients in $\mathbb{Z}$ such that for any $x \in \mathbb{Q}$,

$$x \in \mathbb{Z} \quad \Leftrightarrow \quad (\forall y_1, \ldots, y_n \in \mathbb{Q})(P(x, y_1, \ldots, y_n) \neq 0).$$

In particular, $\mathbb{Z}$ is definable in $\mathbb{Q}$ using only universal quantifiers.

Is $\mathbb{Z}$ existentially definable in $\mathbb{Q}$?: Some heuristic against it

As mentioned previously, it is open whether $\mathbb{Z}$ is existentially definable in $\mathbb{Q}$.

What about subfields K of $\overline{\mathbb{Q}}$ other than $\mathbb{Q}$?

Theorem (Eisenträger, Miller, Springer, Westrick 2020)

In "most" subfields K of $\overline{\mathbb{Q}}$, the ring of integers $\mathcal{O}_K$ is neither existentially definable nor universally definable in K.

Here "most" is measured using Baire category: In order to make this precise one has to define a topology on the space of all subfields of $\overline{\mathbb{Q}}$.

Suggested readings

1. Davis, *Hilbert's tenth problem is unsolvable*
   American Mathematical Monthly, vol. 80, 1973
2. Jones and Matiyasevich, *Proof of recursive unsolvability of Hilbert's tenth problem*
   American Mathematical Monthly, vol. 98, 1991
3. Lagarias, *Succinct certificates for the solvability of binary quadratic Diophantine equations*
   arxiv:math/0611209, 2011 (long version of 1979 FOCS paper).
4. Grunewald and Segal, *How to solve a quadratic equation in integers*
   Mathematical Proceedings of the Cambridge Philosophical Society, vol. 89, 1981.
5. Poonen, *Hilbert's tenth problem over rings of number-theoretic interest*
   Unpublished notes, 2003.
6. Eisenträger, Miller, Springer, and Westrick, *A topological approach to undefinability in algebraic extensions of* $\mathbb{Q}$
   arXiv:2010.09551, 2020.