Hilbert’s 10th problem

Thorsten Altenkirch

David Hilbert (1862-1943)

```
1900
Paris International
Congress
```

Hilbert proposed
23 outstanding problems
in Mathematics

Hilbert’s problems

1a Is there a transfinite number between that of a denumerable set and the numbers of the continuum?
Independent, Cohen 1963

1b Can the continuum of numbers be considered a well ordered set?
Yes, Zermelo 1904 using the Axiom of Choice
which is independent, Fraenkel 1925

2. Can it be proven that the axioms of logic are consistent?
No, Gödel 1931

8. Prove the Riemann hypothesis. Still open

10. Does there exist a universal algorithm for solving Diophantine equations? Topic today

Diophantine equations

Example
Are there solutions $x, y \in \mathbb{Z}$

$$ax + by = 1$$

for $a, b \in \mathbb{Z} - \{0\}$
$a = 10, b = 21$, yes, $x = -2, y = 1$
$a = 6, b = 10$, no

In general?

Relatively Prime

Every number can be (uniquely) represented as a product of primes, e.g.

$$\begin{aligned} 6 &= \\ 10 &= \\ 21 &= \end{aligned}$$

Def.: Two numbers are relatively prime, iff the lists of primes is disjoint.
10 and 21 are relatively prime.
6 and 10 are not relatively prime.
Prop.: $ax + by = 1$ has integer solutions, iff a and b are relatively prime.

Hilbert 10th, revisited

Consider Diophantine equations made up from $\times$ and $+$.
Dioph$(\mathbb{Z})$

Is there a computer program which decides **Dioph**$(\mathbb{Z})$?

Given an equation in **Dioph**$(\mathbb{Z})$ the program would answ

yes if there is a solution

no if there is no solution.

Undecidability

Turing, 1930: *The problem **Halt** to decide whether a given program (Turing machine) halts is undecidable, i.e it cannot be solved by any program (Turing machine).*

Reduction

To show that a problem P is undecidable,
we construct a reduction **Halt** $\leq_m P$,
that is a computer program which translates instances of the halting problem into instances of P.
Why does this work ?

Yuri Matiyasevich (1947)

1971
Matiyasevich shows that
Halt $\leq_m$ **Dioph**$(\mathbb{Z})$

Hence, the answer
to Hilbert's 10th
is negative

Julia Roberts

Halt
$\leq_{\mathrm{Roberts}}$
ExpDioph$\mathbb{Z}$
$\leq_{\mathrm{Matiyasevich}}$
Dioph$(\mathbb{Z})$

ExpDioph

Consider Diophantine equations made up from $\times$ and $+$
and x^y ExpDioph$(\mathbb{Z})$
We will show: **ExpDioph**$(\mathbb{Z})$ is undecidable.

By reducing it to the Halting problem for register machines.

Eliminating $\wedge$

Prop: A conjunction of 2 equations

$$\begin{array}{rrcl} & f(x,y) & = & 0 \\ \wedge & g(x,y) & = & 0 \end{array}$$

can be reduced to one.
How?
Use $f(x,y)^2 + g(x,y)^2 = 0$.

This also works for n equations (and m variables).

Eliminating $\vee$

Prop: A disjunction of 2 equations

$$\begin{array}{rrcl} & f(x,y) & = & 0 \\ \vee & g(x,y) & = & 0 \end{array}$$

can be reduced to one.
How?
Use $f(x,y)g(x,y) = 0$.

This also works for n equations (and m variables).

Eliminating negative numbers

Dioph$(\mathbb{Z}) \simeq_m$ **Dioph**$(\mathbb{N})$

Dioph$(\mathbb{Z}) \leq_m$ **Dioph**$(\mathbb{N})$

How?

$$\exists_{x,y\in\mathbb{Z}} f(x,y) = 0$$
$$\Longleftrightarrow$$
$$\exists_{x,y\in\mathbb{N}} f(x,y) = 0 \vee f(-x,y) = 0$$
$$\vee f(x,-y) = 0 \vee f(-x,-y) = 0$$

Dioph$(\mathbb{N}) \leq_m$ Dioph$(\mathbb{Z})$

Hint
Lagrange: Every natural number can be written as the sum of four squares.

$$\exists_{x,y\in\mathbb{N}} f(x,y) = 0$$
$$\Longleftrightarrow$$
$$\exists_{x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4\in\mathbb{Z}} f(x_1^2+x_2^2+x_3^2+x_4^2, y_1^2+y_2^2+y_3^2+y_4^2) = 0$$

Rest of the talk

We are going to show that **Halt** $\leq_m$ **ExpDioph**$(\mathbb{N})$.
Here **Halt** is the Halting problem for Register machines.
Hence we have shown that **ExpDioph**$(\mathbb{Z})$ is undecidable.
We believe Matiyasevich that **ExpDioph**$(\mathbb{Z}) \leq_m$ **Dioph**$(\mathbb{Z})$

or read his paper.

Register machines

k registers: $R_1, R_2, \ldots R_k$ with values in $\mathbb{N}$. Program:

$$\begin{array}{ccl} 1 & : & A_1 \\ 2 & : & A_2 \\ & \vdots & \\ m & : & A_m \end{array}$$

What are the possible instructions A_i ?

Instructions

- INC R_j (and DEC R_j)
  increments (decrements) register R_j by one.
- GOTO l
  Goto line l.
- IF $R_j = 0$ GOTO l
  Goto line l, if R_j is 0
- HALT
  Ends the program.

Why don't we have $R_j := 0$ or $R_i := R_j$?

$R_j := 0$

```
1 : IF $R_j = 0$ GOTO $4$
2 : DEC $R_j$
3 : GOTO $1$
4 : ...
```

$R_i := R_j$

```
1  : $R_k := 0$
2  : IF $R_j = 0$ GOTO $6$
3  : DEC$R_j$
4  : INC$R_i$
5  : INC$R_k$
6  : IF $R_k = 0$ GOTO $10$
7  : DEC $R_k$
8  : INC $R_j$
9  : GOTO $6$
10 : ...
```

The Halting problem

Given a register machine started with all registers 0, will the machine stop?

We are going to constract a set of equations in **ExpDioph**$(\mathbb{N})$

which has a solution iff the machine stops.

The dominance relation

Def.: $x \trianglelefteq y \iff$ the ith bit of $x \leq$ the ith bit of x
$5 \trianglelefteq 7$, because $5 = 101_2, 7 = 111_2$
$5 \not\trianglelefteq 6$, because $5 = 101_2, 6 = 110_2$

We will see: $\trianglelefteq$ is definable in **ExpDioph**$(\mathbb{N})$

Important Variables

B the largest integer, $B = 2^K$

S the number of steps until HALT

W_j Values of register R_j

$$|\underbrace{W_{j0}}_{K}|\underbrace{W_{j1}}_{K}|\ldots|\underbrace{W_{jS}}_{K}|$$

N_i Sequence number for instruction A_i

$$|\underbrace{N_{i0}}_{K}|\underbrace{N_{i1}}_{K}|\ldots|\underbrace{N_{iS}}_{K}|$$

$N_js = 1 \iff A_i$ is executed at time s
$N_j = 0$ otherwise.

First equations

$$B > k, B > m, B > 2S$$

But these are not equations?

$$B = k + c_1, B = m + c_2, B = 2S + c_3$$

T

$$T = \overbrace{|\underbrace{0\ldots01}_{K}|\underbrace{0\ldots01}_{K}|\ldots|\underbrace{0\ldots01}_{K}|}^{S}$$

$$1 + (B-1)T = B^{S+1}$$

$$N_{is} \in \{0, 1\}$$

$$N_i \trianglelefteq T$$

More equations

- Exactly one instruction is executed at any time.

$$N_1 + N_2 + \cdots + N_m = T$$

- The program starts with the first instruction.

$$1 \trianglelefteq N_1$$

- The last instruction is $A_m = \texttt{HALT}$.

$$B^S \trianglelefteq N_m$$

- Initially all registers are 0.

$$W_j \trianglelefteq B^{S+1} - B$$

i : GOTO j

$$BN_i \trianglelefteq N_j$$

Also for $i : \texttt{INC}\ R_j, i : \texttt{DEC}\ R_j$ we add

$$BN_i \trianglelefteq N_{i+1}$$

INC,DEC

$$\begin{aligned} I_j &= \{i \mid i : \texttt{INC}\ R_j\} \\ D_j &= \{i \mid i : \texttt{DEC}\ R_j\} \end{aligned}$$

$$W_j = B(W_j + \Sigma_{i \in I_j} N_i - \Sigma_{i \in D_j} N_i$$

i : **IF** $R_j = 0$ **GOTO** l

The next step is either $i+1$ or l

$$BN_i \trianglelefteq N_l + N_{i+1}$$

To test $R_j = 0$:

$$BN_i \trianglelefteq N_{i+1} + BT - 2W_j$$

Back to $\trianglelefteq$

Theorem (Kummer,Lucas): $x \trianglelefteq y \iff \binom{y}{x}$ is odd

Hence we replace $x \trianglelefteq y$ by

$$\binom{y}{x} = 2c+1$$

What about $\binom{y}{x}$?

$$\begin{aligned} m = \binom{n}{k} \\ \iff \exists u, v, w . u = 2^n + 1 \wedge v < u^k \wedge m < u \\ \wedge (1+u)^n = wu^{k+1} + mu^k + v \end{aligned}$$