Progress in the formalization of Matiyasevich's theorem in the Mizar system

Karol Pąk

pakkarol@uwb.edu.pl

University of Bialystok,
Institute of Informatics

August 13, 2018

Hilbert's Tenth Problem

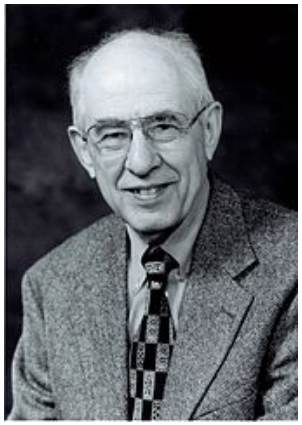
Hilbert's Question

Is there an algorithm which can determine whether or not an arbitrary polynomial equation in several variables has solutions in integers?

Modern formulation

There exists a program taking coefficients of a polynomial equation as input and producing *yes* or *no* answer to the question: *Are there integer solutions?*

The Answer

Martin Davis, Julia Robinson, Yuri Matiyasevich(b. 1947), Hilary Putnam

Negative solution of Hilbert's tenth problem (≈1949–1970)

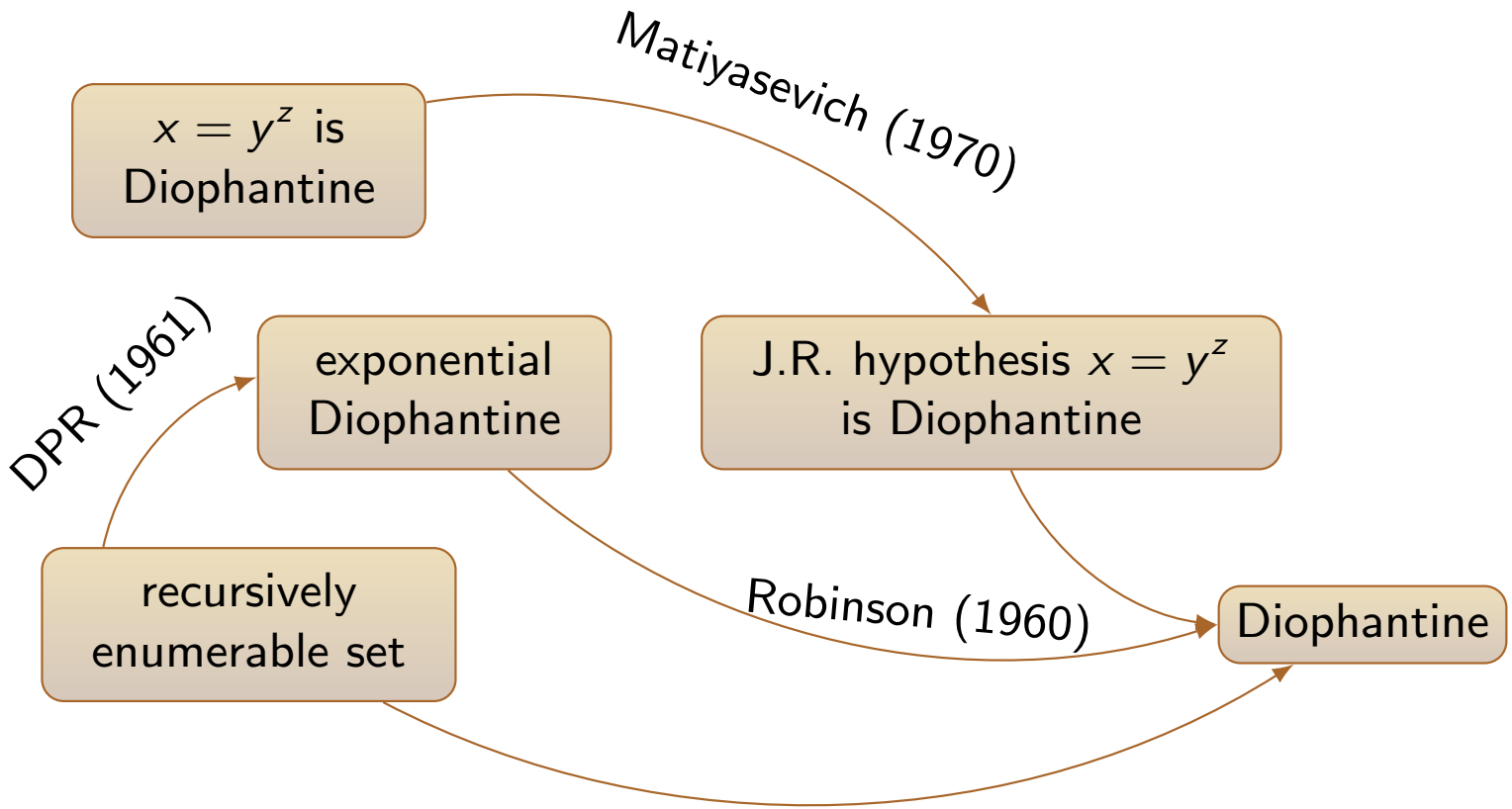
All recursively enumerable sets are Diophantine.

Historical overview

Davis approach (≈1949)

- Hilbert's tenth problem has a negative solution, if
- there is no general algorithm to determine whether a Diophantine equation has solutions in the integers, if
- there exists a Diophantine set that is not recursive, if
- Davis's conjecture is true.

Historical overview



Davis's conjecture (1948)

Normal form for recursively enumerable sets (Martin Davis, 1949)

$$\{a \mid \exists y \forall k \leqslant y \exists x_1, \ldots, x_n : p(a, k, y, x_1, \ldots, x_n) = 0\}$$

Matiyasevich's theorem

Exponentiation is Diophantine i.e. there exists a suitable polynomial P with the property:

$$p = q^r \iff \exists x_1, x_2, \ldots, x_m : P(p, q, r, x1, x2, ..., xm) = 0.$$

The proof technique

- The original approach: From a Diophantine definition of the relation $y = F_{2x}$ where F_0, F_1, F_2, ... are Fibonacci numbers.
- Post–Matiyasevich approach Explores the Pell equation: $x^2 - Dy^2 = 1$.

Selected solutions of Pell's equation

List of the smallest non zero solution to $x^2 - Dy^2 = 1$ for given D:

- $x^2 - 46y^2 = 1$, pair $\langle 24335, 3588 \rangle$.
- $x^2 - 53y^2 = 1$, pair $\langle 66249, 9100 \rangle$.
- $x^2 - 61y^2 = 1$, pair $\langle 1766319049, 226153980 \rangle$.
- $x^2 - 73y^2 = 1$, pair $\langle 2281249, 267000 \rangle$.

Question: Is there always a solution?

Selected solutions of Pell's equation

List of the smallest non zero solution to $x^2 - Dy^2 = 1$ for given D:

- $x^2 - 46y^2 = 1$, pair $\langle 24335, 3588 \rangle$.
- $x^2 - 53y^2 = 1$, pair $\langle 66249, 9100 \rangle$.
- $x^2 - 61y^2 = 1$, pair $\langle 1766319049, 226153980 \rangle$.
- $x^2 - 73y^2 = 1$, pair $\langle 2281249, 267000 \rangle$.

Question: Is there always a solution?
Answer: Yes (Joseph-Louis Lagrange 1768).

Selected solutions of Pell's equation

List of the smallest non zero solution to $x^2 - Dy^2 = 1$ for given D:

- $x^2 - 46y^2 = 1$, pair $\langle 24335, 3588 \rangle$.
- $x^2 - 53y^2 = 1$, pair $\langle 66249, 9100 \rangle$.
- $x^2 - 61y^2 = 1$, pair $\langle 1766319049, 226153980 \rangle$.
- $x^2 - 73y^2 = 1$, pair $\langle 2281249, 267000 \rangle$.

Question: Is there always a solution?
Answer: Yes (Joseph-Louis Lagrange 1768).

Formalizing 100 Theorems (Freek Wiedijk)

39. Solutions to Pell's Equation
    HOL Light, John Harrison
    Mizar, Marcin Acewicz & Karol Pak
    Metamath, Stefan O'Rear

Pell's equation in Mizar

$N 39. Solutions to Pell's Equation

```
theorem :: PELLS_EQ:14
  D is non square implies
    ex x,y be Nat st x^2 - D * y^2 = 1 & y <> 0;
```

$N The Cardinality of the Pell's Solutions

```
theorem :: PELLS_EQ:17
  for D be non square Nat holds
    the set of all ab where ab is positive
      Pell's_solution of D is infinite;
```

Post-Matiyasevich approach

- Based on a special case (easy case) of the Pell's equation that has the form $x^2 - (a^2 - 1)y^2 = 1$.
- Solutions of the case can be ordered in two sequences recursively:

$$\begin{aligned} x_0(a) &= 1 \\ y_0(a) &= 0 \\ x_{n+1}(a) &= a \cdot x_n(a) + (a^2 - 1) \cdot y_n(a) \\ y_{n+1}(a) &= x_n(a) + a \cdot y_n(a) \end{aligned}$$

Post-Matiyasevich approach - First *advanced* lemma

theorem :: HILB10_1:38
  for y,z,a be Nat holds
    y = Py(a,z) & a > 1 iff

Post-Matiyasevich approach - First *advanced* lemma

```
theorem :: HILB10_1:38
  for y,z,a be Nat holds
      y = Py(a,z) & a > 1 iff
  ex x,x1,y1,A,x2,y2 be Nat st
    a>1 &
    [x,y] is Pell's_solution of (a^2- 1) &
    [x1,y1] is Pell's_solution of (a^2- 1) &
    y1>=y & A > y & y >= z &
    [x2,y2] is Pell's_solution of (A^2- 1) &
    y2,y are_congruent_mod x1 &
    A,a are_congruent_mod x1 &
    y2,z are_congruent_mod 2*y &
    A,1 are_congruent_mod 2*y &
    y1,0 are_congruent_mod y^2;
```

Post-Matiyasevich approach - Second *advanced* lemma

```
theorem :: HILB10_1:39
    for x,y,z be Nat holds
        y = x|^z
    iff
      (y = 1 & z = 0) or
      (x = 0 & y = 0 & z > 0) or
      (x = 1 & y = 1 & z > 0) or
      (x > 1 & z > 0 & ex y1,y2,y3,K be Nat st
           y1 = Py(x,z+1) & K > 2*z*y1 &
           y2 = Py(K,z+1) & y3 = Py(K*x,z+1) &
           (0 <= y-y3/y2 <1/2 or 0 <= y3/y2 -y < 1/2));
```

Diophantine set

A Diophantine set is a subset A of $\mathbb{N}^i$ for some i such that there exists j and a polynomial equation with integer coefficients and unknowns $P(x, y) = 0$ with $x \in \mathbb{N}^i$, $y \in \mathbb{N}^j$ such that

$$\forall_{a \in \mathbb{N}^i}\ a \in A \iff \exists_{b \in \mathbb{N}^j} P(a, b) = 0.$$

```
definition
  let n be Nat;
  let A be Subset of n -xtuples_of NAT;
  attr A is diophantine means :: HILB10_2:def 6
    ex m being Nat,p being INT-valued Polynomial of n+m,F_Real st
      for s holds
            s in A iff ex x being n-element XFinSequence of NAT,
                       y being m-element XFinSequence of NAT st
                         s = x & eval(p,@(x^y)) = 0;
end;
```

Matiyasevich's piece of the puzzle

theorem HILB10_3:23
for i1,i2,i3 be Element of n holds
{p where p be n-element XFinSequence of NAT:
p.i1 = Py(p.i2,p.i3) & p.i2 > 1}
is diophantine Subset of n -xtuples˙of NAT

theorem HILB10_3:24
for i1,i2,i3 be Element of n holds
{p where p be n-element XFinSequence of NAT:
p.i2 =(p.i1) |^ (p.i3)}
is diophantine Subset of n -xtuples˙of NAT

Proof overview

Intersections and unions of Diophantine sets are Diophantine.

Proof. Suppose $P1(T, X)$, $P2(T, Y)$ are polynomials that determine subsets $A1$ and $A2$, respectively. Then

$$P1(T, X) \cdot P2(T, Y), \;\; P1(T, X)^2 + P2(T, Y)^2$$

are suitable polynomials to determine $A1 \cup A2$, $A1 \cap A2$.

Substitution

If $R \subset \omega^{n+1}$ is Diophantine and F is an n-ary function with a Diophantine graph, then the relation $S(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ defined by

$$S : R(x_0, \ldots, x_{i-1}, F(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n), x_{i+1}, \ldots, x_n)$$

is also Diophantine.

Substitution in Mizar

```
scheme Substitution{P[Nat,Nat,Nat,Nat,Nat,Nat],
  F(Nat,Nat,Nat)→Nat}:
    for i1,i2,i3,i4,i5 holds {p: P[p.i1,p.i2,F(p.i3,p.i4,p.i5),p.i3,p.i4,p.i5]}
      is diophantine Subset of n -xtuples_of NAT
provided
  A1: for i1,i2,i3,i4,i5,i6 holds {p: P[p.i1,p.i2,p.i3,p.i4,p.i5,p.i6]}
    is diophantine Subset of n -xtuples_of NAT
and
  A2:for i1,i2,i3,i4 holds {p: F(p.i1,p.i2,p.i3) = p.i4}
    is diophantine Subset of n -xtuples_of NAT
```

DPRM Theorem – current state

Probably one of the last advanced lemma

If $R \subset \omega^{n+2}$ is Diophantine then $\forall_{y \leqslant x}\{a | a^\frown \langle x, y\rangle \in R\}$ is Diophantine.

DPRM Theorem – current state

Probably one of the last advanced lemma

If $R \subset \omega^{n+2}$ is Diophantine then $\forall_{y \leqslant x}\{a | a^\frown\langle x, y\rangle \in R\}$ is Diophantine.

2.11. Bounded Quantifier Theorem. *Let* $P(A_0, ..., A_{m-1}, X, Y, X_0, ..., X_{n-1})$ *be a polynomial. There is a polynomial* $Q(A_0, ..., A_{m-1}, X)$ *such that, for any* $a_0, ..., a_{m-1} \in \omega$,

i. $\forall x\, [Q(a_0, ..., a_{m-1}, x) \geq x]$

ii. $\forall x\, \forall y x_0 ... x_{n-1} \leq x\, [|P(\boldsymbol{a}, x, y, \boldsymbol{x})| \leq Q(\boldsymbol{a}, x)]$

iii. *for any x, the following are equivalent:*

a. $\forall y \leq x\, \exists x_0 ... x_{n-1} \leq x\, [P(\boldsymbol{a}, x, y, \boldsymbol{x}) = 0]$

b. $$\exists c t v_0 ... v_{n-1}\, [t = Q(\boldsymbol{a},x)! \wedge 1 + (c+1)t = \prod_{m=0}^{x}(1 + (m+1)t) \wedge$$
$$\wedge\ 1 + (c+1)t \mid \prod_{j=0}^{x}(v_0 - j) \wedge ... \wedge 1 + (c+1)t \mid \prod_{j=0}^{x}(v_{n-1} - j) \wedge$$
$$\wedge\ 1 + (c+1)t \mid P(a_0, ..., a_{m-1}, x, c, v_0, ..., v_{n-1})].$$

Proof technique

Chinese remainder theorem, 4 combinatorial lemmas: binomial is Diophantine and further factorial, two cases of product.

Currently up to the 4-th lemma

```
theorem step4:
    for x,y,x1 be Nat st x1 >= 1holds
      y = Product (1+(x1 * idseq x))
    iff
      ex u,w,y1,y2,y3,y4,y5 be Nat st
          u > y & x1*w,1 are˙congruent˙mod u &
          y1 = x1|^x &
          y2 = x! &
          y3 = (w+x) choose x &
          y1*y2*y3,y are_congruent_mod u &
          y4 = 1+x1*x &
          y5 = y4|^x & u > y5
```

Conclusions

- 4 Mizar articles, 8600–lines.
- 1 goal from Freek Wiedijk's list of "Top 100 mathematical theorems".
- Matiyasevich's theorem (piece of the puzzle).