Using Ideas in Matiyasevich's Seminal Proof of the Undecidability of the General Diophantine Equation in order to concoct lots and lots of Decidable Ones

Robert DOUGHERTY-BLISS, Charles KENNEY, and Doron ZEILBERGER

Abstract: We extract ideas implicit in Matiyasevich's (negative) resolution of Hilbert's tenth problem, to construct many non-trivial infinite families for which we can not just decide that they have solutions, but in fact explicitly construct all the solutions. We can also come up with many families for which we can prove that no solutions exist.

Preface

In 1970, 23-year-old Yuri Matiyasevich, standing on the shoulders of Julia Robinson, Martin Davis, and Hilary Putnam, shocked the world of mathematics by showing that David Hilbert's dream of finding an algorithm that inputs *any* polynomial

$$P(x_1, \dots, x_n)$$

with integer coefficients, and outputs **true** or **false** if $P = 0$ has, or does not have, solutions in integers, can never come to be.

Of course, for *specfic* equations, and even, many specific infinite families, one can often decide, but there is no *magic bullet* that, can decide all of them.

For example, Pythagoras got very upset when Hippasus of Metapontum discovered that the diophantine equation

$$x^2 - 2y^2 = 0 \quad ,$$

has **no solution**, and Hippasus (probably) gave a fully rigorous proof (**not** the usual one but a geometrical version of the **reduction formula** if (x, y) $x > y > 0$ is a solution so is $(y, 2x - y$ and since $(1, 0)$ is not a solution **qed**. Going backwards, using the fact that if (x, y) is a solution of *Pell's equation*

$$x^2 - 2y^2 \ = \ \pm 1$$

then so is $(x + 2y, x + y)$, we can prove that there are **infinitely many** solutions. A little more effort will show that these are the only ones. (see [Z]).

Much harder is the fact proved by Sir Andrew Wiles [W], that for every $n > 2$ the diophantine equation

$$x^n + y^n = z^n \quad ,$$

has no solution.

On the positive side, Noam Elkies [E] famously proved that

$$A^4 + B^4 + C^4 = D^4 \quad ,$$

has *infinitely* many solutions.

Wouldn't it be nice to be able to manufacture, *at will*, many examples of diophantine equations for which we can explicitly construct *all solutions* (and prove that these are the only ones), and also construct many equations for which we can conclusively assert that they have **no solutions**.

A cheap way to manufacture diophantine equations with infinitely many solutions

As most of us know, the triple

$$a = A^2 - B^2 \quad , \quad , b = 2AB \quad , \quad c = A^2 + B^2 \quad ,$$

satisfies

$$a^2 + b^2 = c^2$$

(check!) A little more challenging is to prove that all solutions of $a^2 + b^2 = c^2$ with $gcd(a, b) = 1$ are of this form. This gives a cheap way to manufacture many examples of diophantine equations for which we know that there infinitely many solutions (and in fact know how to solve them).

Take any $m + 1$ polynomials in m variables with integer coefficients

$$P_i(a_1, \ldots, a_m) \quad , \quad 1 \leq i \leq m + 1$$

and define

$$X_i = P_i(a_1, \ldots, a_m) \quad , \quad 1 \leq i \leq m + 1 \quad ,$$

using, e.g **Gröbner bases** (the Buchberger algorithm) we can *eliminate* $a_1, \ldots, a_m$ and get a polynomial equation (with integer coefficients)

$$Q(X_1, \ldots, X_m) \, = \, 0 \quad ,$$

that has a parametric solution as above. Alas, in general this leads to monster equations and unlike the case with Pythagorean triples, it is not clear that they aren't other solutions.

So it would be nice to be able to generate, in a systematic way, many examples of simple diophantine equations for which we know infinitely many solutions, and to be able to prove that these are all of them. It would also be nice to manufacture not too complicated, but non-trivial, diophantine equations for which we can conclusively prove that there aren't any solutions.

Matiyasevich's seminal proof

In Matiyasevich's proof (we use the versions in [JM] and [M]) a central role is played by *Pell's equation* and the fact ([M], pp. 19-20) that two consecutive terms $x = a_b(n), y = a_b(n + 1)$ of the sequence of integers defined by the **second-order** linear recurrence

$$a_b(0) = 0 \quad , \quad a_b(1) = 1 \quad , \quad a_b(n + 2) \, = \, b a_b(n + 1) - a_b(n) \quad ,$$

satisfy the diophantine equation

$$x^2 - bxy + y^2 = 1 \quad ,$$

and conversely if $x > y$ satisfies it, then there must be an n such that $x = a_b(n+1)$, $y = a_b(n)$.

This gave us the idea to consider higher-order recurrences, and see what happens.

Maple package

This article is accompanied by a Maple package `Hilbert10.txt` available from the front of this article

`https://sites.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/hilbert10.html` ,

that also has links to numerous sample output files with lots and lots of nice diophantine equations for which we can find *all* solutions, and rigorously prove that these are the only ones. See for example the output file

`https://sites.math.rutgers.edu/~zeilberg/tokhniot/oHilbert10e.txt` .

References

[E] Noam Elkies, *on* $A^4 + B^4 + c^4 = D^4$, Mathematics of Computation **51** (1988), 825-835.

[JM] J. P. Jones and Y.V. Matiyasevich, *Proof of recursive unsolvability of Hilbert's tenth problem*, Amer. Math. Monthly **98** (1991), 689-709.

[M] Yuri V. Matiyasevich, *"Hilbert's Tenth Problem"*, The MIT Press, 1993.

[W] Andrew Wiles, *Modular Elliptic Curves and Fermat's Last Theorem*, Annals of Mathematics Second Series, **141**(3) (May, 1995), 443-551.

[Z] Doron Zeilberger, *Two Motivated Concrete Proofs (much better than the usual one) that the Square-Root of 2 is Irrational*, The Personal Journal of Shalosh B. Ekhad and Doron Zeilberger. `https://sites.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/sqrt2.html` .

Robert Dougherty-Bliss , Department of Mathematics, Rutgers University (New Brunswick), Hill Center-Busch Campus, 110 Frelinghuysen Rd., Piscataway, NJ 08854-8019, USA.
Email: `robert dot w dot bliss at gmail dot com` .

Charles T. Kenney, Department of Mathematics, Rutgers University (New Brunswick), Hill Center-Busch Campus, 110 Frelinghuysen Rd., Piscataway, NJ 08854-8019, USA.
Email: `ctk47 at rutgers dot edu` .

Doron Zeilberger, Department of Mathematics, Rutgers University (New Brunswick), Hill Center-Busch Campus, 110 Frelinghuysen Rd., Piscataway, NJ 08854-8019, USA.
Email: `DoronZeil at gmail dot com` .

First written: Dec. 25, 2023; This version: Dec. 25, 2023.