 doi:10.20944/preprints201902.0156.v4

Diophantine equations with a finite number of solutions: Craig Smoryński's theorem, Harvey Friedman's conjecture, and relative recursive enumerability

Apoloniusz Tyszka

Abstract

Matiyasevich's theorem states that there is no algorithm to decide whether or not a given Diophantine equation has a solution in non-negative integers. Smoryński's theorem states that the set of all Diophantine equations which have at most finitely many solutions in non-negative integers is not recursively enumerable. We prove: (1) Smoryński's theorem easily follows from Matiyasevich's theorem, (2) Hilbert's Tenth Problem for $\mathbb{Q}$ has a negative solution if and only if the set of all Diophantine equations with a finite number of rational solutions is not recursively enumerable, (3) the question of whether or not a given Diophantine equation has at most finitely many integer solutions is semi-decidable with an oracle that decides whether or not a given Diophantine equation has an integer solution.

Key words and phrases: Davis-Putnam-Robinson-Matiyasevich theorem, Diophantine equation which has at most finitely many solutions, Hilbert's Tenth Problem, Hilbert's Tenth Problem for $\mathbb{Q}$, Matiyasevich's theorem, oracle that decides whether or not a given Diophantine equation has an integer solution, oracle that decides whether or not a given Diophantine equation has a rational solution, recursively enumerable set, relative recursive enumerability.

1 Introduction

The Davis-Putnam-Robinson-Matiyasevich theorem states that every recursively enumerable set $\mathcal{M} \subseteq \mathbb{N}$ has a Diophantine representation; that is

$$a \in \mathcal{M} \Longleftrightarrow \exists x_1, \ldots, x_m \in \mathbb{N} \;\; W(a, x_1, \ldots, x_m) = 0 \qquad \text{(R)}$$

for some polynomial W with integer coefficients, see [7]. The representation (R) is said to be infinite-fold if for every $a \in \mathcal{M}$ the equation $W(a, x_1, \ldots, x_m) = 0$ has infinitely many solutions $(x_1, \ldots, x_m) \in \mathbb{N}^m$. A stronger version of the Davis-Putnam-Robinson-Matiyasevich theorem states that each recursively enumerable subset of $\mathbb{N}$ has an infinite-fold Diophantine representation with 9 variables, see [4], [6], [7, p. 163], and [9, p. 243].

Martin Davis' theorem states that the set of all Diophantine equations which have at most finitely many solutions in positive integers is not recursive, see [1]. Craig Smoryński's theorem states that the set of all Diophantine equations which have at most finitely many solutions in non-negative integers is not recursively enumerable, see [8, p. 104, Corollary 1] and [9, p. 240]. Yuri Matiyasevich's theorem states that there is no algorithm to decide whether or not a given Diophantine equation has a solution in non-negative integers ([7]). The same is true for solutions in integers and for solutions in positive integers ([7]).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 March 2019 doi:10.20944/preprints201902.0156.v4

Matiyasevich's theorem easily follows from the Davis-Putnam-Robinson-Matiyasevich theorem without the use of Smoryński's theorem ([7]). Similarly, the stronger version of the Davis-Putnam-Robinson-Matiyasevich theorem implies that Matiyasevich's theorem holds for Diophantine equations which have at most k variables, where $k \geqslant 9$, see [7]. In section 3, we show that Smoryński's theorem easily follows from Matiyasevich's theorem. In section 4, we show that Hilbert's Tenth Problem for $\mathbb{Q}$ has a negative solution if and only if the set of all Diophantine equations with a finite number of rational solutions is not recursively enumerable.

2 Basic lemmas

Let $\mathcal{P}$ denote the set of prime numbers, and let

$$\mathcal{P} = \{p_1, q_1, r_1, p_2, q_2, r_2, p_3, q_3, r_3, \ldots\},$$

where $p_1 < q_1 < r_1 < p_2 < q_2 < r_2 < p_3 < q_3 < r_3 < \ldots$.

Lemma 1. *For a non-negative integer x, let $\prod_{i=1}^{\infty} p_i^{\alpha_i} \cdot q_i^{\beta_i} \cdot r_i^{\gamma_i}$ be the prime decomposition of $x+1$. For every positive integer n, the mapping which sends $x \in \mathbb{N}$ into*

$$\left((-1)^{\alpha_1} \cdot \frac{\beta_1}{\gamma_1 + 1}, \ldots, (-1)^{\alpha_n} \cdot \frac{\beta_n}{\gamma_n + 1}\right) \in \mathbb{Q}^n$$

is a computable surjection from $\mathbb{N}$ onto $\mathbb{Q}^n$.

Lemma 2. *A Diophantine equation $D(x_1, \ldots, x_p) = 0$ has no solutions in non-negative integers (alternatively, integers, positive integers, rationals) $x_1, \ldots, x_p$ if and only if the equation $D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} = 0$ has at most finitely many solutions in non-negative integers (respectively, integers, positive integers, rationals) $x_1, \ldots, x_{p+1}$.*

Proof. We present the proof for solutions in non-negative integers. Let $\mathcal{A}_1$ denote the following statement: *A Diophantine equation $D(x_1, \ldots, x_p) = 0$ has no solutions in non-negative integers $x_1, \ldots, x_p$.* Let $\mathcal{A}_2$ denote the following statement: *The equation $D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} = 0$ has at most finitely many solutions in non-negative integers $x_1, \ldots, x_{p+1}$.* We need to prove that

$$(\mathcal{A}_1 \Rightarrow \mathcal{A}_2) \wedge (\mathcal{A}_2 \Rightarrow \mathcal{A}_1)$$

We present the proof that $\mathcal{A}_1$ implies $\mathcal{A}_2$. The statement $\mathcal{A}_1$ implies that the set of all tuples $(x_1, \ldots, x_{p+1}) \in \mathbb{N}^{p+1}$ which satisfy $D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} = 0$ is empty. The empty set is finite. We present the proof that $\mathcal{A}_2$ implies $\mathcal{A}_1$. Assume, on the contrary, that non-negative integers $a_1, \ldots, a_p$ satisfy $D(a_1, \ldots, a_p) = 0$. Then,

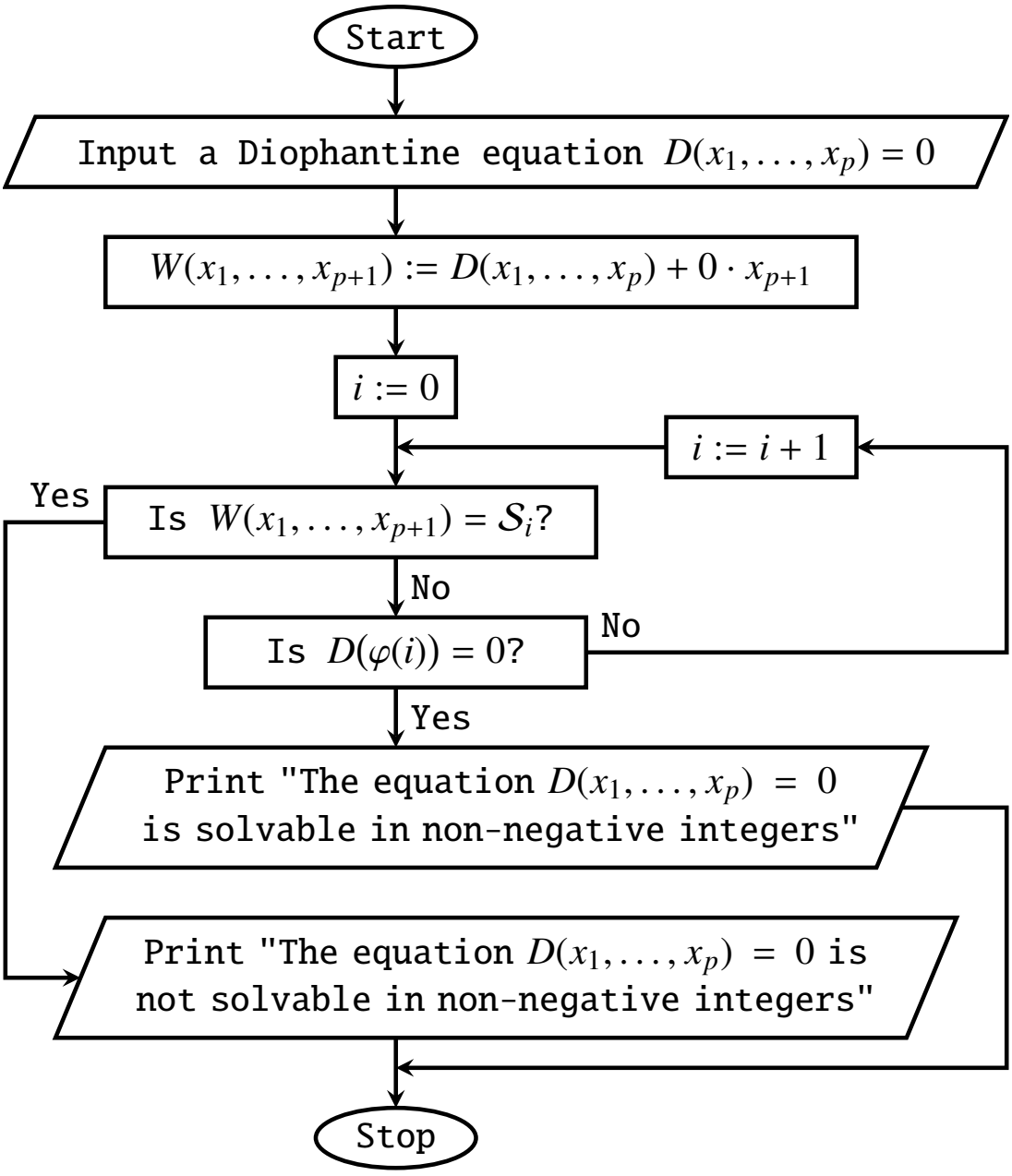
$$\forall x_{p+1} \in \mathbb{N} \;\; D(a_1, \ldots, a_p) + 0 \cdot x_{p+1} = 0$$

Therefore, infinitely many tuples $(x_1, \ldots, x_{p+1}) \in \mathbb{N}^{p+1}$ solve the equation $D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} = 0$, a contradiction. The proof for solutions in integers (positive integers, rationals) is analogous. □

Lemma 3. *If the set of all Diophantine equations which have at most finitely many solutions in non-negative integers (alternatively, integers, positive integers, rationals) is recursively enumerable, then there exists an algorithm which decides whether or not a given Diophantine equation has a solution in non-negative integers (respectively, integers, positive integers, rationals).*

Proof. We present the proof for solutions in non-negative integers. Suppose that $\{\mathcal{S}_i = 0\}_{i=0}^{\infty}$ is a computable sequence of all Diophantine equations which have at most finitely many solutions in non-negative integers. By Lemma 2, the execution of Flowchart 1 decides whether or not a Diophantine equation $D(x_1, \ldots, x_p) = 0$ has a solution in non-negative integers. The flowchart algorithm uses a computable surjection $\varphi\colon \mathbb{N} \to \mathbb{N}^p$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 March 2019 doi:10.20944/preprints201902.0156.v4



Flowchart 1

The flowchart algorithm always terminates because there exists a non-negative integer i such that

$$(D(x_1,\ldots,x_p)+0\cdot x_{p+1}=\mathcal{S}_i)\vee(D(\varphi(i))=0)$$

Indeed, for every Diophantine equation $D(x_1,\ldots,x_p)=0$, the flowchart algorithm finds a solution in non-negative integers, or finds the equation $D(x_1,\ldots,x_p)+0\cdot x_{p+1}=0$ on the infinite list $[\mathcal{S}_0,\mathcal{S}_1,\mathcal{S}_2,\ldots]$ if the equation $D(x_1,\ldots,x_p)=0$ is not solvable in non-negative integers.

For solutions in integers, we choose a computable surjection $\varphi\colon\mathbb{N}\to\mathbb{Z}^p$, modify the definition of the sequence $\{\mathcal{S}_i=0\}_{i=0}^{\infty}$, and modify the two print instructions. For solutions in positive integers, we choose a computable surjection $\varphi\colon\mathbb{N}\to(\mathbb{N}\setminus\{0\})^p$, modify the definition of the sequence $\{\mathcal{S}_i=0\}_{i=0}^{\infty}$, and modify the two print instructions. For solutions in rationals, we apply Lemma 1 and choose a computable surjection $\varphi\colon\mathbb{N}\to\mathbb{Q}^p$, modify the definition of the sequence $\{\mathcal{S}_i=0\}_{i=0}^{\infty}$, and modify the two print instructions. □

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 March 2019 doi:10.20944/preprints201902.0156.v4

3 The set of all Diophantine equations which have at most finitely many solutions in non-negative integers is not recursively enumerable

Theorem 1. *The set of all Diophantine equations which have at most finitely many solutions in non-negative integers (integers, positive integers) is not recursively enumerable.*

Proof. It follows from Lemma 3 and Matiyasevich's theorem. □

Let $\mathcal{E}$ denote the set of all Diophantine equations $D(x_1, \ldots, x_p) = 0$ such that $p \in \mathbb{N} \setminus \{0\}$ and the polynomial $D(x_1, \ldots, x_p)$ truly depends on all the variables $x_1, \ldots, x_p$. The last phrase means that for every $i \in \{1, \ldots, p\}$ the polynomial $D(x_1, \ldots, x_p)$ involves a non-zero monomial which is divided by x_i, if $D(x_1, \ldots, x_p)$ is written as the sum of a minimal number of monomials.

Lemma 4. *A Diophantine equation $D(x_1, \ldots, x_p) = 0$ has no solutions in non-negative integers $x_1, \ldots, x_p$ if and only if the equation $\left(2x_{p+1} + 1\right) \cdot D(x_1, \ldots, x_p) = 0$ has at most finitely many solutions in non-negative integers $x_1, \ldots, x_{p+1}$.*

Lemma 5. *If a polynomial $D(x_1, \ldots, x_p) \in \mathbb{Z}[x_1, \ldots, x_p]$ truly depends on all the variables $x_1, \ldots, x_p$, then the polynomial $\left(2x_{p+1} + 1\right) \cdot D(x_1, \ldots, x_p)$ truly depends on all the variables $x_1, \ldots, x_{p+1}$.*

Theorem 2. *The equations which belong to $\mathcal{E}$ and which have at most finitely many solutions in non-negative integers form a set which is not recursively enumerable.*

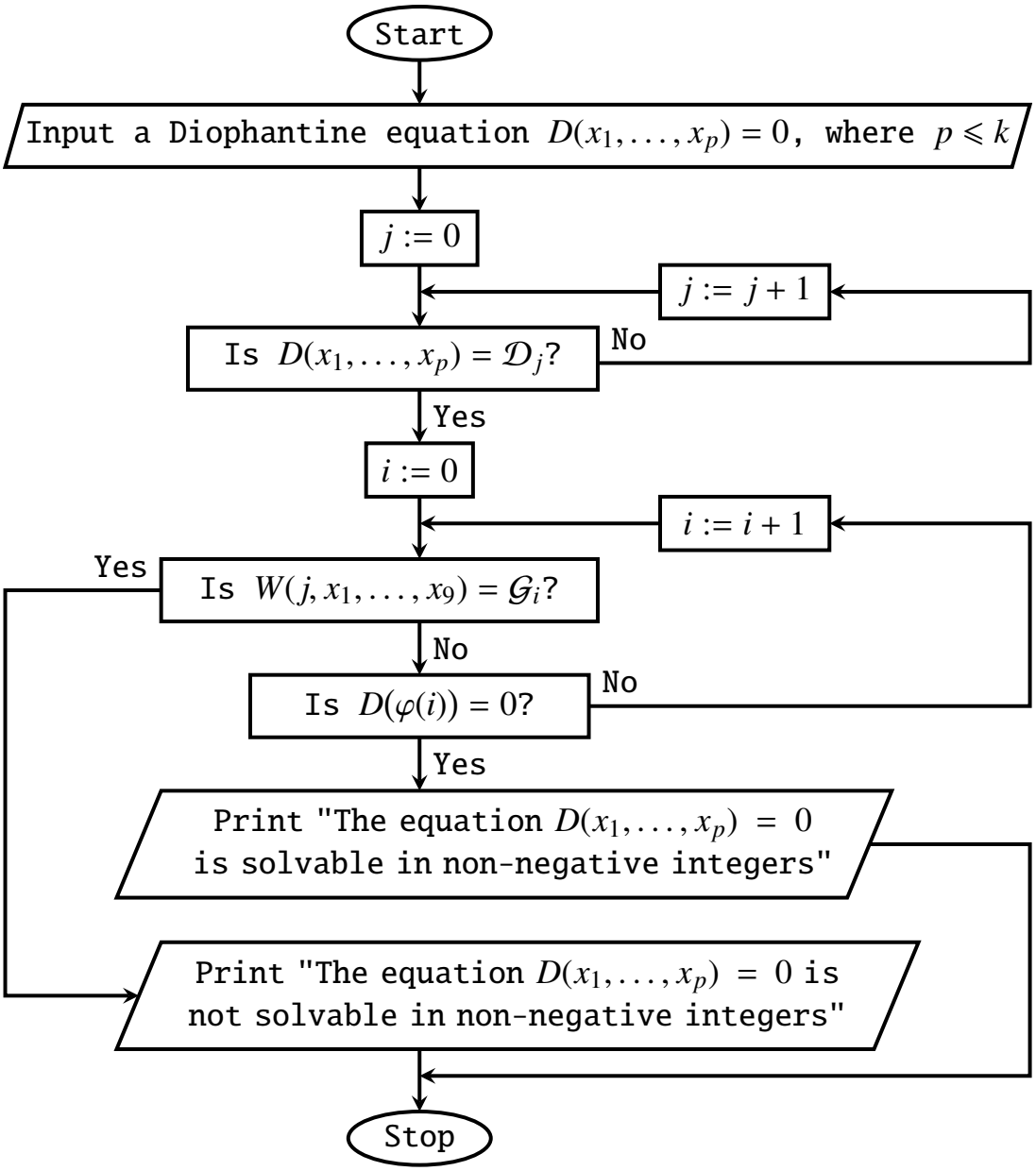
Proof. We reformulate Lemma 3 for Diophantine equations which belong to $\mathcal{E}$. The proof, which uses Lemmas 3–5, is analogous to the proof of Theorem 1. □

For a positive integer k, let $Dioph(k)$ denote the set of all Diophantine equations which have at most k variables and at most finitely many solutions in non-negative integers.

Theorem 3. *For every integer $k \geqslant 9$, the set $Dioph(k)$ is not recursively enumerable.*

Proof. Let $\{D_j = 0\}_{j=0}^{\infty}$ be a computable sequence of all Diophantine equations which have at most k variables. By the stronger version of the Davis-Putnam-Robinson-Matiyasevich theorem, there exists a polynomial $W(x, x_1, \ldots, x_9) \in \mathbb{Z}[x, x_1, \ldots, x_9]$ such that for every non-negative integer j, the equation $D_j = 0$ is solvable in non-negative integers if and only if the equation $W(j, x_1, \ldots, x_9) = 0$ has infinitely many solutions in non-negative integers $x_1, \ldots, x_9$. Equivalently, for every non-negative integer j, the equation $D_j = 0$ has no solutions in non-negative integers if and only if the equation $W(j, x_1, \ldots, x_9) = 0$ has at most finitely many solutions in non-negative integers $x_1, \ldots, x_9$. Suppose, on the contrary, that $\{\mathcal{G}_i = 0\}_{i=0}^{\infty}$ is a computable sequence of all equations from $Dioph(k)$. Then, the execution of Flowchart 2 decides whether or not a Diophantine equation $D(x_1, \ldots, x_p) = 0$ (where $p \leqslant k$) has a solution in non-negative integers $x_1, \ldots, x_p$. The flowchart algorithm uses a computable surjection $\varphi\colon \mathbb{N} \to \mathbb{N}^p$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 March 2019 doi:10.20944/preprints201902.0156.v4



Flowchart 2

Thus we have a contradiction to Matiyasevich's theorem. The flowchart algorithm always terminates because there exist non-negative integers i and j such that

$$(D(x_1, \ldots, x_p) = \mathcal{D}_j) \wedge ((W(j, x_1, \ldots, x_9) = \mathcal{G}_i) \vee (D(\varphi(i)) = 0))$$

□

4 Hilbert's Tenth Problem for $\mathbb{Q}$

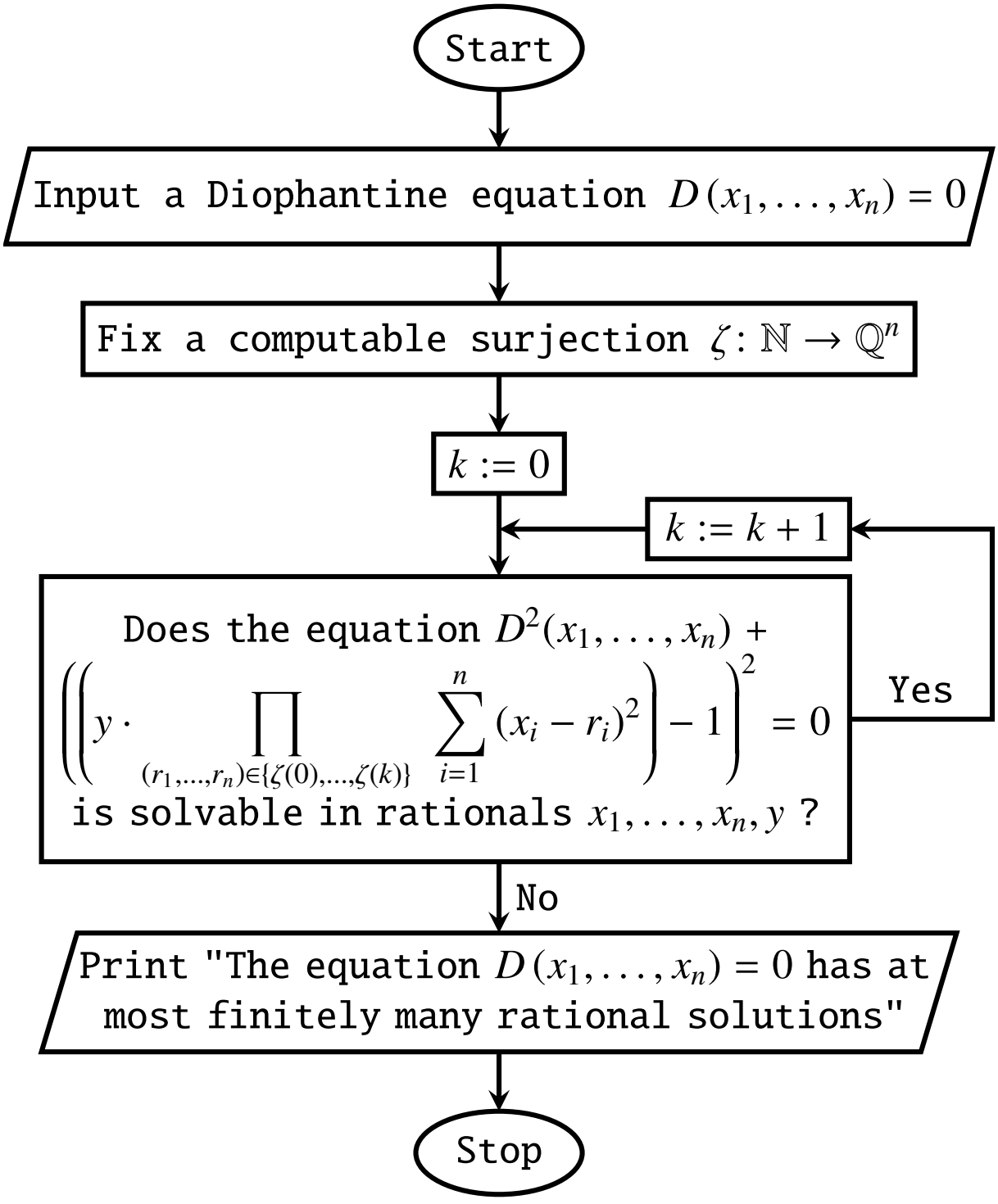
Hilbert's Tenth Problem for $\mathbb{Q}$ remains unsolved, see [2] and [7]. Harvey Friedman conjectures that the set of all Diophantine equations which have only finitely many rational solutions is not recursively enumerable, see [3]. For solutions in rationals, Lemma 3 claims that a negative solution to Hilbert's Tenth Problem for $\mathbb{Q}$ implies that the set of all Diophantine equations with a finite number of rational solutions is not recursively enumerable. We show the converse implication.

Lemma 6. *For every rational number b, $b \neq 0$ if and only if the equation $y \cdot b - 1 = 0$ is solvable in rationals.*

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 March 2019 doi:10.20944/preprints201902.0156.v4

Theorem 4. *A positive solution to Hilbert's Tenth Problem for $\mathbb{Q}$ implies that the set of all Diophantine equations with a finite number of rational solutions is recursively enumerable.*

Proof. We assume a positive solution to Hilbert's Tenth Problem for $\mathbb{Q}$. By Lemma 6, the algorithm in Flowchart 3 halts if and only if a Diophantine equation $D(x_1, \ldots, x_n) = 0$ has at most finitely many rational solutions.



Flowchart 3

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 March 2019 doi:10.20944/preprints201902.0156.v4

We explain in details why the algorithm in Flowchart 3 is correct. For a non-negative integer k, let $W_k(x_1, \ldots, x_n, y) = 0$ be the equation

$$D^2(x_1, \ldots, x_n) + \left(\left(y \cdot \prod_{(r_1, \ldots, r_n) \in \{\zeta(0), \ldots, \zeta(k)\}} \sum_{i=1}^{n} (x_i - r_i)^2 \right) - 1 \right)^2 = 0$$

Its coefficients are rational, and they all can be computed. Therefore, for every $k \in \mathbb{N}$, we can compute a positive integer d_k such that the equivalent equation $d_k \cdot W_k(x_1, \ldots, x_k, y) = 0$ has integer coefficients. □

Guess ([5, p. 16]). *The question of whether or not a given Diophantine equation has at most finitely many rational solutions is decidable with an oracle that decides whether or not a given Diophantine equation has a rational solution.*

Originally, Minhyong Kim formulated the Guess as follows: for rational solutions, the finiteness problem is decidable relative to the existence problem.

5 Hilbert's Tenth Problem for subrings of $\mathbb{Q}$

Let R be a subring of $\mathbb{Q}$. We do not assume that $1 \in R$. Let m denote the smallest integer in $(\mathbb{N} \setminus \{0\}) \cap R$. Then, $m \cdot \mathbb{Z} \subseteq R$.

Theorem 5. *We assume that for every positive integer n there exists a computable surjection from $\mathbb{N}$ onto R^n. We claim: if the set of all Diophantine equations which have at most finitely many solutions in R is recursively enumerable, then there exists an algorithm which decides whether or not a given Diophantine equation has a solution in R.*

Proof. The proof is analogous to the proof of Lemma 3. □

Lemma 7. *For every $b \in R$, $b \neq 0$ if and only if the equation*

$$y \cdot b - m^2 - \sum_{i=1}^{4} y_i^2 = 0$$

is solvable in $y, y_1, y_2, y_3, y_4 \in R$.

Proof. If $b = 0$, then for every $y, y_1, y_2, y_3, y_4 \in R$,

$$y \cdot b - m^2 - \sum_{i=1}^{4} y_i^2 = -m^2 - \sum_{i=1}^{4} y_i^2 < 0$$

If $b \in R$ and $b < 0$, then $b = \frac{p}{q}$, where $p \in (-\infty, -1] \cap \mathbb{Z}$ and $q \in \mathbb{N} \setminus \{0\}$. In this case, for $y = -m^2 \cdot q \in R$ we have $y \cdot b = -m^2 \cdot p \in m^2 \cdot (\mathbb{N} \setminus \{0\})$. If $b \in R$ and $b > 0$, then $b = \frac{p}{q}$, where $p, q \in \mathbb{N} \setminus \{0\}$. In this case, for $y = m^2 \cdot q \in R$ we have $y \cdot b = m^2 \cdot p \in m^2 \cdot (\mathbb{N} \setminus \{0\})$. In both cases, by Lagrange's four-square theorem, there exist $t_1, t_2, t_3, t_4 \in \mathbb{N}$ such that

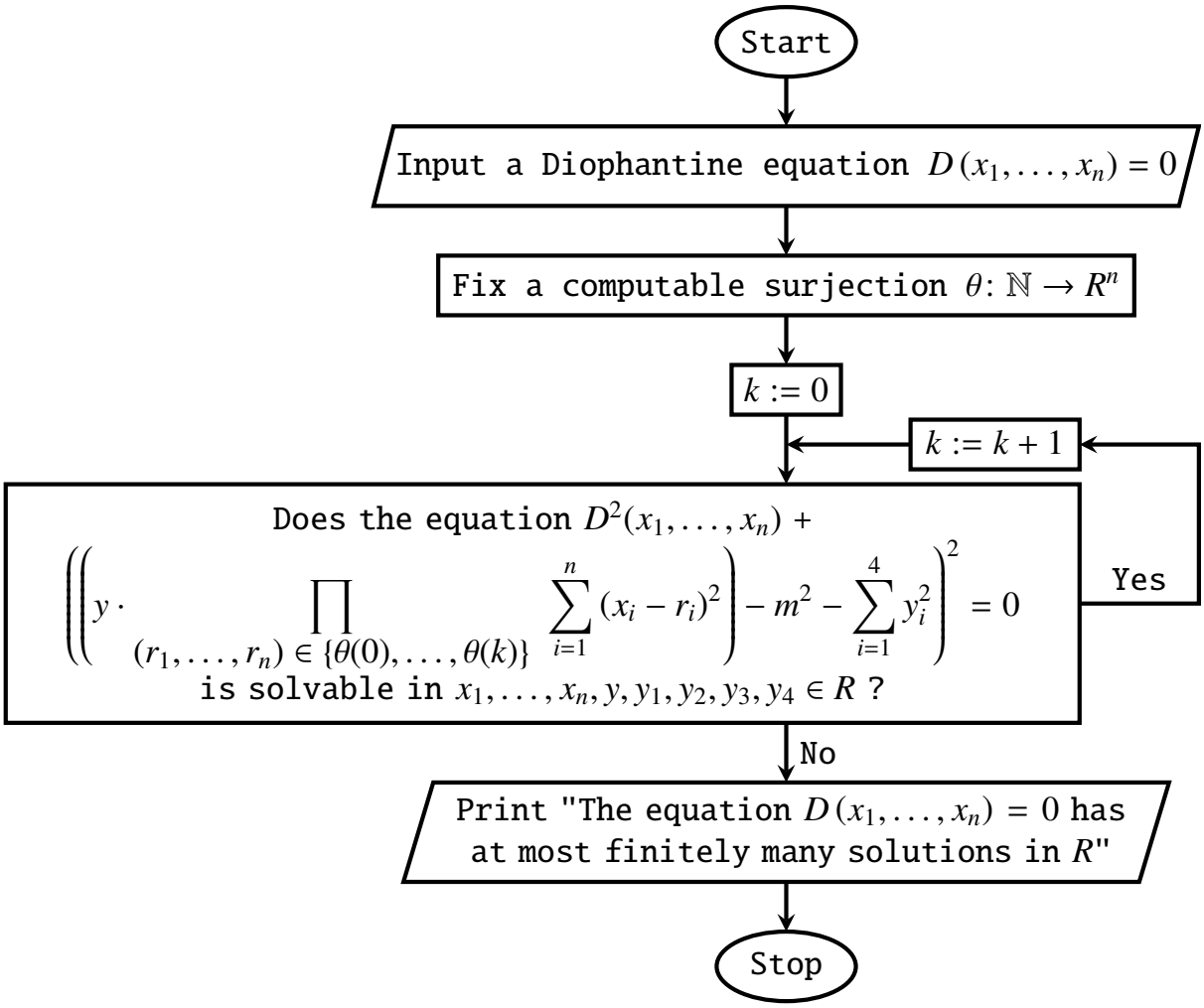
$$\frac{y \cdot b - m^2}{m^2} = t_1^2 + t_2^2 + t_3^2 + t_4^2$$

Hence, $y \cdot b - m^2 - (m \cdot t_1)^2 - (m \cdot t_2)^2 - (m \cdot t_3)^2 - (m \cdot t_4)^2 = 0$, where $m \cdot t_1,\ m \cdot t_2,\ m \cdot t_3,\ m \cdot t_4 \in R$. □

Theorem 6. *We assume that for every positive integer n there exists a computable surjection from $\mathbb{N}$ onto R^n. We claim: a positive solution to Hilbert's Tenth Problem for R implies that the set of all Diophantine equations with a finite number of solutions in R is recursively enumerable.*

Proof. We assume a positive solution to Hilbert's Tenth Problem for R. By Lemma 7, the algorithm in Flowchart 4 halts if and only if a Diophantine equation $D(x_1, \ldots, x_n) = 0$ has at most finitely many solutions in R.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 March 2019 doi:10.20944/preprints201902.0156.v4



Flowchart 4

□

6 The question of whether or not a given Diophantine equation has at most finitely many integer solutions is semi-decidable with an oracle that decides whether or not a given Diophantine equation has an integer solution

Lemma 8. *([10, p. 177]). For every integer b, $b\neq 0$ if and only if the equation*

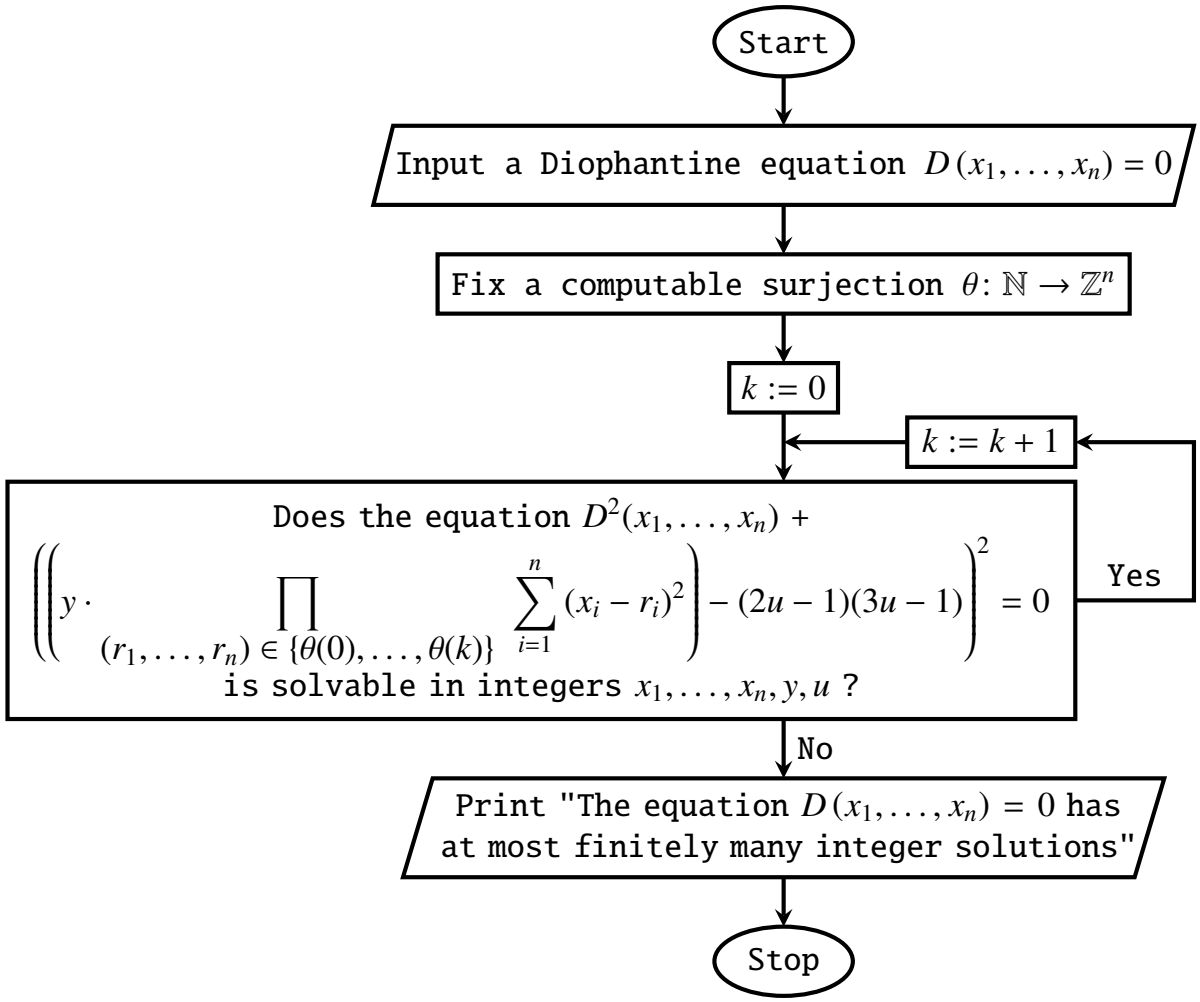
$$y\cdot b-(2u-1)(3u-1)=0$$

is solvable in integers.

Theorem 7. *The question of whether or not a given Diophantine equation has at most finitely many integer solutions is semi-decidable with an oracle that decides whether or not a given Diophantine equation has an integer solution.*

Proof. By Lemma 8, the algorithm in Flowchart 5 halts if and only if a Diophantine equation $D(x_1,\ldots,x_n)=0$ has at most finitely many integer solutions.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 March 2019 doi:10.20944/preprints201902.0156.v4



Flowchart 5

By the Davis-Putnam-Robinson-Matiyasevich theorem, the oracle in the claim of the theorem decides the halting problem. This strong argument makes the proof trivial and without the use of Lemma 8. □

References

[1] M. Davis, *On the number of solutions of Diophantine equations*, Proc. Amer. Math. Soc. 35 (1972), no. 2, 552–554, http://doi.org/10.1090/S0002-9939-1972-0304347-1.

[2] M. Davis, *Representation theorems for recursively enumerable sets and a conjecture related to Poonen's large subring of* $\mathbb{Q}$, J. Math. Sci. (N.Y.) 171 (2010), no. 6, 728–730, http://doi.org/10.1007/s10958-010-0176-7.

[3] H. Friedman, *Complexity of statements,* April 20, 1998, http://www.cs.nyu.edu/pipermail/fom/1998-April/001843.html.

[4] J. P. Jones, *Universal Diophantine equation*, J. Symbolic Logic 47 (1982), no. 3, 549–571, http://doi.org/10.2307/2273588.

[5] M. Kim, *On relative computability for curves,* Asia Pac. Math. Newsl. 3 (2013), no. 2, 16–20, http://www.asiapacific-mathnews.com/03/0302/0016_0020.pdf.

[6] Yu. Matiyasevich, *Some purely mathematical results inspired by mathematical logic,* in: Proceedings of Fifth International Congress on Logic, Methodology and Philosophy of Science, London, Ontario, 1975, Reidel, Dordrecht, 1977, 121-127, http://doi.org/10.1007/978-94-010-1138-9_7.

[7] Yu. Matiyasevich, *Hilbert's tenth problem,* MIT Press, Cambridge, MA, 1993.

[8] C. Smoryński, *A note on the number of zeros of polynomials and exponential polynomials,* J. Symbolic Logic 42 (1977), no. 1, 99–106, http://doi.org/10.2307/2272324.

[9] C. Smoryński, *Logical number theory, vol. I,* Springer, Berlin, 1991.

[10] A. Tyszka, *Two conjectures on the arithmetic in* $\mathbb{R}$ *and* $\mathbb{C}$, MLQ Math. Log. Q. 56 (2010), no. 2, 175–184, http://doi.org/10.1002/malq.200910004.

Apoloniusz Tyszka
University of Agriculture
Faculty of Production and Power Engineering
Balicka 116B, 30-149 Kraków, Poland
E-mail: rttyszka@cyf-kr.edu.pl