Hilbert's 10th Problem for solutions in a subring of Q

Agnieszka Peszek, Apoloniusz Tyszka

Hilbert's 10th Problem for solutions in a subring of $\mathbb{Q}$

Agnieszka Peszek, Apoloniusz Tyszka

Abstract

Yuri Matiyasevich's theorem states that the set of all Diophantine equations which have a solution in non-negative integers is not recursive. 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. Let R be a subring of $\mathbb{Q}$ with or without 1. By $H_{10}(R)$, we denote the problem of whether there exists an algorithm which for any given Diophantine equation with integer coefficients, can decide whether or not the equation has a solution in R. We prove that a positive solution to $H_{10}(R)$ implies that the set of all Diophantine equations with a finite number of solutions in R is recursively enumerable. We show the converse implication for every infinite set $R \subseteq \mathbb{Q}$ such that there exist computable functions $\tau_1, \tau_2 \colon \mathbb{N} \to \mathbb{Z}$ which satisfy $(\forall n \in \mathbb{N}\ \tau_2(n) \neq 0) \wedge \left(\left\{\frac{\tau_1(n)}{\tau_2(n)} : n \in \mathbb{N}\right\} = R\right)$. This implication for $R = \mathbb{N}$ guarantees that Smoryński's theorem follows from Matiyasevich's theorem. Harvey Friedman conjectures that the set of all polynomials of several variables with integer coefficients that have a rational solution is not recursive. Harvey Friedman conjectures that the set of all polynomials of several variables with integer coefficients that have only finitely many rational solutions is not recursively enumerable. These conjectures are equivalent by our results for $R = \mathbb{Q}$.

2010 Mathematics Subject Classification: 03D25, 11U05.

Key words and phrases: Craig Smoryński's theorem, Diophantine equation which has at most finitely many solutions, Hilbert's 10th Problem for solutions in a subring of $\mathbb{Q}$, Martin Davis' theorem, recursive set, recursively enumerable set, Yuri Matiyasevich's theorem.

1 Introduction and basic lemmas

Yuri Matiyasevich's theorem states that the set of all Diophantine equations which have a solution in non-negative integers is not recursive, see [3]. 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 [4, p. 104, Corollary 1] and [5, p. 240].

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 $x \in \mathbb{N}$ to*

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

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

Let $s_n \colon \mathbb{N} \to \mathbb{Q}^n$ denote the surjection defined in Lemma 1.

Lemma 2. *For every infinite set $R \subseteq \mathbb{Q}$, a Diophantine equation $D(x_1, \ldots, x_n) = 0$ has no solutions in $x_1, \ldots, x_n \in R$ if and only if the equation $D(x_1, \ldots, x_n) + 0 \cdot x_{n+1} = 0$ has at most finitely many solutions in $x_1, \ldots, x_{n+1} \in R$.*

Let R be a subring of $\mathbb{Q}$ with or without 1. By $H_{10}(R)$, we denote the problem of whether there exists an algorithm which for any given Diophantine equation with integer coefficients, can decide whether or not the equation has a solution in R.

2 A positive solution to $H_{10}(R)$ implies that the set of all Diophantine equations with a finite number of solutions in R is recursively enumerable

In the next three lemmas we assume that $\{0\} \subsetneq R \subseteq \mathbb{Q}$ and $r \cdot \mathbb{Z} \subseteq R$ for every $r \in R$. Every non-zero subring R of $\mathbb{Q}$ (with or without 1) satisfies these conditions.

Lemma 3. *There exists a non-zero integer $m \in R$.*

Proof. There exist $m, n \in \mathbb{Z} \setminus \{0\}$ such that $\frac{m}{n} \in R$. Hence, $m = \frac{m}{n} \cdot n \in (\mathbb{Z} \setminus \{0\}) \cap R$. □

Lemma 4. *Let $m \in (\mathbb{Z} \setminus \{0\}) \cap R$. We claim that 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 $y, y_1, y_2, y_3, y_4 \in R$,

$$y \cdot b - m^2 - y_1^2 - y_2^2 - y_3^2 - y_4^2 = -m^2 - y_1^2 - y_2^2 - y_3^2 - y_4^2 \leqslant -m^2 < 0$$

If $b \neq 0$, then $b = \frac{p}{q}$, where $p \in \mathbb{N} \setminus \{0\}$ and $q \in \mathbb{Z} \setminus \{0\}$. In this case, we define y as $m^2 \cdot q$ and observe that $m^2 \cdot q = (m \cdot q) \cdot m \in R$ as $m \cdot q \in R$ and $m \in \mathbb{Z}$. Hence,

$$y \cdot b = (m^2 \cdot q) \cdot \frac{p}{q} = m^2 \cdot p \in m^2 \cdot (\mathbb{N} \setminus \{0\})$$

By Lagrange's four-square theorem, there exist $t_1, t_2, t_3, t_4 \in \mathbb{N}$ such that

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

Therefore,

$$y \cdot b - m^2 - (m \cdot t_1)^2 - (m \cdot t_2)^2 - (m \cdot t_3)^2 - (m \cdot t_4)^2 = 0,$$

where $m \cdot t_1,\ m \cdot t_2,\ m \cdot t_3,\ m \cdot t_4 \in R$. □

Lemma 5. *We can uniquely express every rational number r as $\widehat{r} \,/\, \overline{r}$, where $\widehat{r} \in \mathbb{Z}$, $\overline{r} \in \mathbb{N} \setminus \{0\}$, and the integers $\widehat{r}$ and $\overline{r}$ are relatively prime. If $r \in R$, then $\widehat{r} \in R$.*

Proof. For every $r \in R$, $\widehat{r} = r \cdot \overline{r} \in r \cdot \mathbb{Z} \subseteq R$. □

Lemma 6. *Let R be a non-zero subring of $\mathbb{Q}$ with or without 1. We claim that for every $T_0, \ldots, T_k \in R^n$ and for every $x_1, \ldots, x_n \in R$, the following product*

$$\prod_{(r_1, \ldots, r_n) \in \{T_0, \ldots, T_k\}} \sum_{i=1}^{n} (x_i \cdot \overline{r_i} - \widehat{r_i})^2 \tag{1}$$

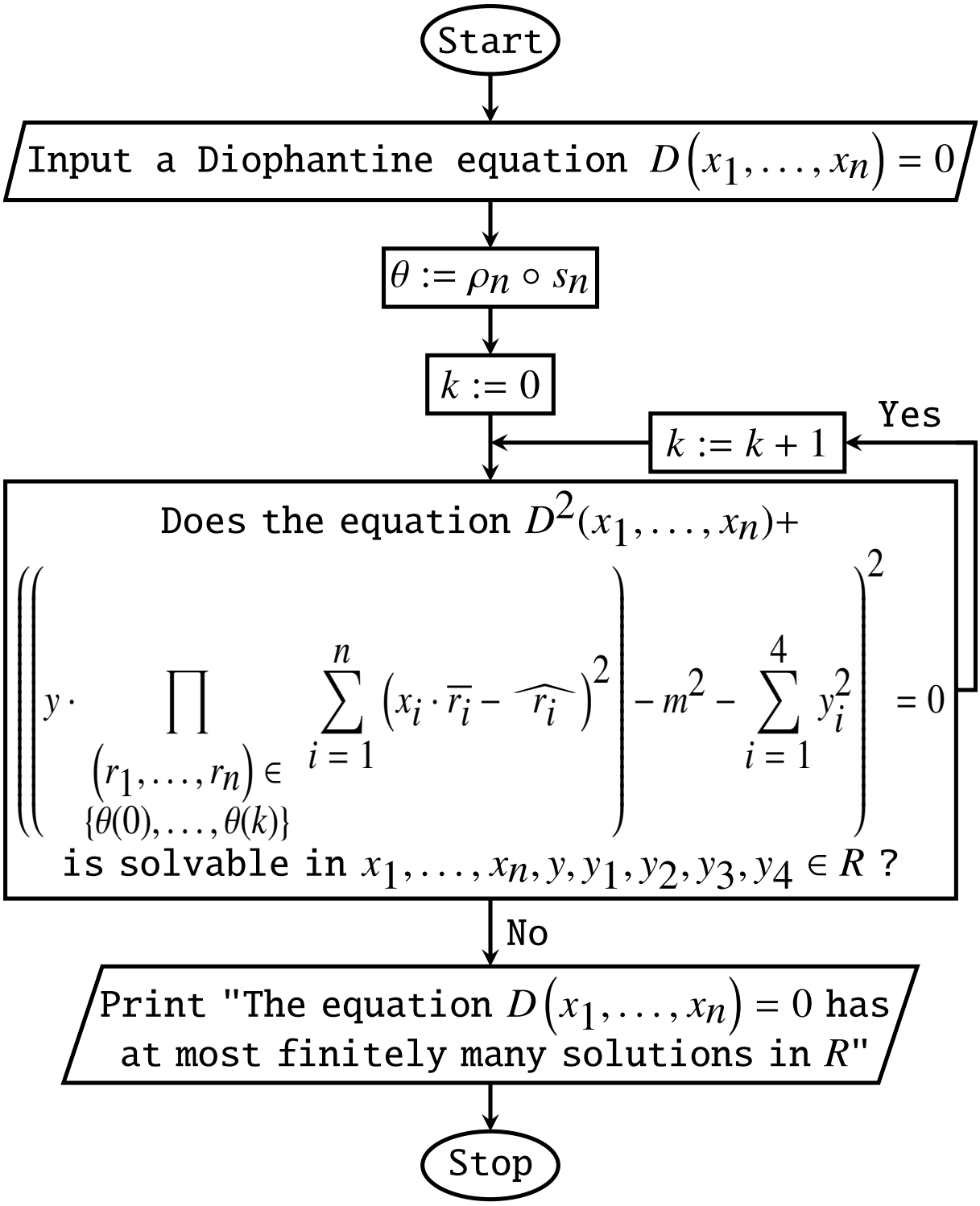
differs from 0 if and only if $(x_1, \ldots, x_n) \notin \{T_0, \ldots, T_k\}$. Product (1) belongs to R.

Proof. The last claim follows from Lemma 5. □

Lemma 7. *Let R be a non-zero subring of $\mathbb{Q}$ (with or without 1) such that there exists an algorithm which for every $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ decides whether or not $\frac{a}{b} \in R$. Let $\rho_n \colon \mathbb{Q}^n \to R^n$ denote the function which equals the identity on R^n and equals $(0, \ldots, 0)$ outside R^n. We claim that for every positive integer n the function $\rho_n \circ s_n \colon \mathbb{N} \to R^n$ is surjective and computable.*

Theorem 1. *Let R be a non-zero subring of $\mathbb{Q}$ (with or without 1) such that Hilbert's 10th Problem for solutions in R has a positive solution. We claim that the set of all Diophantine equations with a finite number of solutions in R is recursively enumerable.*

Proof. By Lemma 3, there exists a non-zero integer $m \in R$. For every $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, the solvability in R of the equation $b \cdot x - a = 0$ is decidable. Hence, for every $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ we can decide whether or not $\frac{a}{b} \in R$. By Lemmas 4 and 6, the answer to the question in Flowchart 1 is positive if and only if the equation $D(x_1, \ldots, x_n) = 0$ is solvable in $R^n \setminus \{\theta(0), \ldots, \theta(k)\}$. Hence, by Lemma 7, the algorithm in Flowchart 1 halts if and only if the equation $D(x_1, \ldots, x_n) = 0$ has at most finitely many solutions in R.



Flowchart 1

□

Theorem 1 remains true when $R=\{0\}$. The flowchart algorithm depends on $m\in(\mathbb{Z}\setminus\{0\})\cap R$. For a constructive proof of Theorem 1, we must compute an element of $(\mathbb{Z}\setminus\{0\})\cap R$. By Lemma 7, the function $\rho_n\circ s_n\colon\mathbb{N}\to R^n$ is computable and surjective. We compute the smallest $i\in\mathbb{N}$ such that $(\rho_n\circ s_n)(i)$ starts with a non-zero integer. This integer belongs to $(\mathbb{Z}\setminus\{0\})\cap R$.

3 If the set of all Diophantine equations with a finite number of solutions in R is recursively enumerable, then $H_{10}(R)$ has a positive solution

Starting from this moment up to the end of Theorem 2, we assume that R is an infinite subset of $\mathbb{Q}$ and there exist computable functions $\tau_1, \tau_2 \colon \mathbb{N} \to \mathbb{Z}$ which satisfy

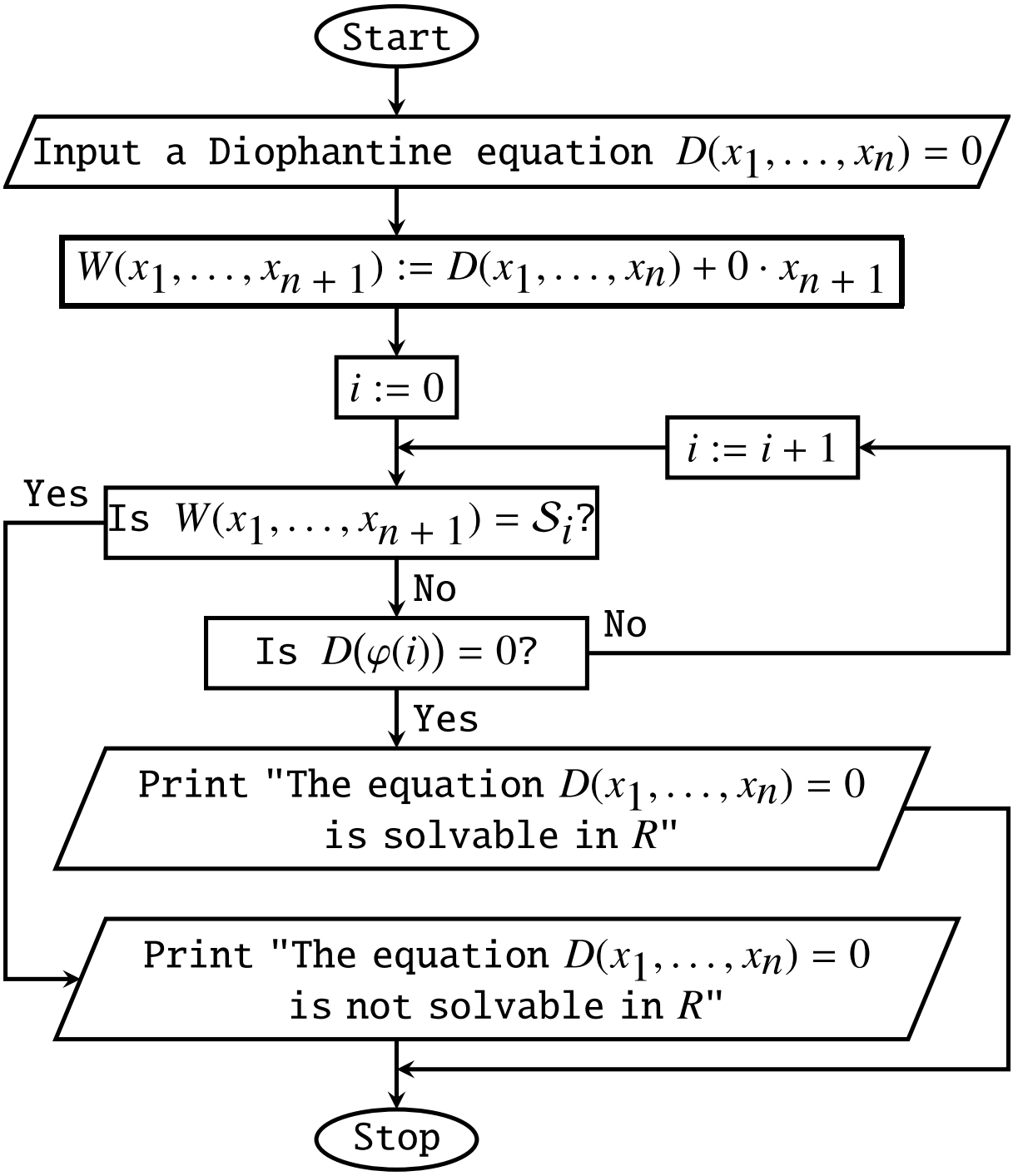
$$(\forall n \in \mathbb{N}\ \tau_2(n) \neq 0) \wedge \left(\left\{ \frac{\tau_1(n)}{\tau_2(n)} \ :\ n \in \mathbb{N} \right\} = R \right)$$

In other words, the function $\mathbb{N} \ni n \xrightarrow{\tau} \frac{\tau_1(n)}{\tau_2(n)} \in R$ is surjective and computable. Hence, the function $(\tau, \ldots, \tau) : \mathbb{N}^n \to R^n$ is surjective and computable.

Lemma 8. *Let $\sigma_n \colon \mathbb{Q}^n \to \mathbb{N}^n$ denote the function which equals the identity on $\mathbb{N}^n$ and equals $(0, \ldots, 0)$ outside $\mathbb{N}^n$. We claim that for every positive integer n the function $(\tau, \ldots, \tau) \circ \sigma_n \circ s_n \colon \mathbb{N} \to R^n$ is surjective and computable.*

Theorem 2. *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. Suppose that $\{S_i = 0\}_{i=0}^{\infty}$ is a computable sequence of all Diophantine equations which have at most finitely many solutions in R. By Lemma 2, the execution of Flowchart 2 decides whether or not a Diophantine equation $D(x_1, \ldots, x_n) = 0$ has a solution in R. The flowchart algorithm uses a computable surjection $\varphi \colon \mathbb{N} \to R^n$ (which exists by Lemma 8).



Flowchart 2

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

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

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

Corollary. *Theorem 2 for $R = \mathbb{N}$ implies that Craig Smoryński's theorem follows from Yuri Matiyasevich's theorem.*

Harvey Friedman conjectures that the set of all polynomials of several variables with integer coefficients that have a rational solution is not recursive, see [2]. Harvey Friedman conjectures that the set of all polynomials of several variables with integer coefficients that have only finitely many rational solutions is not recursively enumerable, see [2]. These conjectures are equivalent by Theorems 1 and 2 taking $R = \mathbb{Q}$.

Acknowledgement. Agnieszka Peszek prepared two flowcharts in *TikZ*. Apoloniusz Tyszka wrote the article. The article was presented at the Jubilee Congress for the 100th anniversary of the Polish Mathematical Society held in Kraków, Poland, September 3-7, 2019. An older and longer version of this article appeared in Scientific Annals of Computer Science 29 (2019), no. 1, 101–111, http://www.info.uaic.ro/en/sacs_articles/on-the-relationship-between-matiyasevichs-and-smorynskis-theorems/. The article's DOI 10.7561/SACS.2019.1.101 does not link to the article.

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

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

[4] 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.

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

Agnieszka Peszek
University of Agriculture
Faculty of Production and Power Engineering
Balicka 116B, 30-149 Kraków, Poland
E-mail: Agnieszka.Peszek@urk.edu.pl

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